TWO DEFINITIONS OF AN ABELIAN GROUP BY SETS OF INDEPENDENT POSTULATES*

BY

EDWARD V. HUNTINGTON

The following definitions of an Abelian (commutative) group are suggested immediately by the writer's definitions of a general group published in the Bulletin of the American Mathematical Society, ser. 2, vol. 8 (1901–1902), pp. 296–300, 388–391.†

§ 1. First definition: by three postulates.

A set of elements in which a rule of combination $\circ$ is so defined as to satisfy the following three postulates shall be called an Abelian group with respect to $\circ$:

1) $a \circ b = b \circ a$, *whenever* a, b *and* $b \circ a$ *belong to the set.*

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

3) *For every two elements* a *and* b $(a = b$ *or* $a \neq b)$ *there is an element* x *in the set such that* $a \circ x = b$.

If we wish to distinguish between finite and infinite groups we may add a fourth postulate, either

a) *The set contains n elements;* or

b) *The set is infinite.*

Familiar examples of a finite and an infinite Abelian group are the following:

A) The system of the first n positive integers, with the rule of combination defined as follows:

$$\begin{aligned} a \circ b &= a + b \qquad \text{when} \qquad a + b \leqq n, \\ &= a + b - n \qquad \text{when} \qquad a + b > n. \end{aligned}$$

B) The system of all integers, positive, negative and zero, with $a \circ b = a + b$; or the system of all positive rational numbers, with $a \circ b = a \times b$.

* Presented to the Society October 25, 1902. Received for publication October 4, 1902.

† Cf. E. H. Moore, Transactions, vol. 3 (1902), pp. 485–492. Professor Moore's criticism of "multiple statements" suggested the present form of postulates 1 and 2.

The following theorems, deduced from postulates 1, 2, 3, show that the present definition is equivalent to the definitions usually given.*

THEOREM I. *The element x in 3 is uniquely determined by a and b.*

Proof. Suppose $a \circ x = b$ and also $a \circ x' = b$; and by 3 take ξ so that $x \circ \xi = x'$. Then by hypothesis $a \circ (x \circ \xi) = b$; or, by 2, $(a \circ x) \circ \xi = b$; or, $b \circ \xi = b$. Now by 3 and 1 take η so that $\eta \circ b = x$. Then $\eta \circ (b \circ \xi) = x$; or, by 2, $(\eta \circ b) \circ \xi = x$; or, $x \circ \xi = x$. Therefore $x = x'$.

COROLLARY. If $a \circ b = a \circ b'$ then $b = b'$.

THEOREM II. *There is a peculiar element e in the set, such that $b \circ e = b$ for every element b.*

Proof. Take any element a and by 3 take e so that $a \circ e = a$; the element e thus determined (Theorem I) is the peculiar element required. For, let b be any other element than a, and by 3 and 1 take x so that $x \circ a = b$. Then $x \circ (a \circ e) = b$; or, by 2, $(x \circ a) \circ e = b$; or $b \circ e = b$.

THEOREM III. *Whenever a and b belong to the set, $a \circ b$ also belongs to the set.*

Proof. By 3 and 1 there is an element b' such that $b' \circ b = e$ and also an element c such that $c \circ b' = a$. Then $c = a \circ b$. For, by 3 take β so that $a \circ \beta = c$ and β' so that $\beta \circ \beta' = e$. Then

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

by 2; hence $b' = \beta'$. Then $b' \circ \beta = \beta' \circ \beta = e = b' \circ b$ by 1; hence $\beta = b$. Therefore $a \circ b = c$.

Independence of postulates 1, 2, 3 and a), when $n > 2$.

The mutual independence of postulates 1, 2, 3 and a), when $n > 2$,† is shown by the following systems, each of which satisfies all the other postulates but not the one for which it is numbered.

(1) The system of the first n positive integers, with $a \circ b = b$.

(2) The system of the first n positive integers, with the rule of combination defined as follows:

$$\begin{array}{llll} & a \circ b = a + b & \text{when} & a + b \leqq n, \\ & \quad = a + b - n & \text{when} & a + b > n; \\ \text{except that} & a \circ b = 2 & \text{when} & a + b = n + 1, \\ \text{and} & a \circ b = 1 & \text{when} & a + b = 2 \text{ or } n + 2. \end{array}$$

(3) The system of the first n positive integers, with $a \circ b = 1$.

(a) Any infinite Abelian group, such as B) above.

* The proofs of these theorems become, of course, much simpler if we confine ourselves to finite groups.

† When $n = 1$, postulate 3 is sufficient. When $n = 2$, postulates 1 and 3 are sufficient and independent.

Independence of postulates 1, 2, 3 and b).

Similarly, the independence of postulates 1, 2, 3 and b) is shown by the following systems:

[1] The system of all positive integers, with $a \circ b = b$.

[2] The system of all rational numbers, with $a \circ b = (a+b)/2$.

[3] The system of all positive integers, with $a \circ b = 1$.

[b] Any finite Abelian group, such as A) above.

§2. Second definition: by four postulates.

An Abelian group may be defined also by the following four postulates:

1′) $a \circ b = b \circ a$, *whenever* $a, b, a \circ b$ *and* $b \circ a$ *all belong to the set.*

2′) $(a \circ b) \circ c = a \circ (b \circ c)$, *whenever* $a, b, c, a \circ b, b \circ c, (a \circ b) \circ c$ *and* $a \circ (b \circ c)$ *all belong to the set.*

3′) *For every two elements* a *and* b ($a = b$ *or* $a \neq b$) *there is an element* x' *in the set such that* $(a \circ x') \circ b = b$.

4′) *If* a *and* b *belong to the set, then* $a \circ b$ *also belongs to the set.*

To show that this second definition agrees with the first, we have only to notice that the truth of 3 follows at once from 2′, 3′, 4′. ($x = x' \circ b$.)

Independence of postulates 1′, 2′, 3′, 4′ and a), when $n > 2$.

The independence of these postulates for finite groups, when $n > 2$,* is established by the use of the following systems:

(1′), (2′), (3′), (a). Same as the systems (1), (2), (3), (a) above.

(4′) The system of the first n positive integers, with the rule of combination defined as follows: $a \circ a = 1$; $1 \circ b = b$; otherwise $a \circ b = z$, an object not belonging to the set.

Independence of postulates 1′, 2′, 3′, 4′ and b).

Similarly, the independence of these postulates for infinite groups is shown by the following systems:

[1′], [2′], [3′], [b]. Same as the systems [1], [2], [3], [b] above.

[4′] The system of all integers except ± 1, with $a \circ b = a + b$.

Harvard University, Cambridge, Mass.,
August, 1902.

* When $n = 1$, postulate 4′ is sufficient. When $n = 2$, postulates 1′, 3′, 4′ are sufficient and independent.

Postscript.*

In the course of an article entitled *A Definition of Abstract Groups*,† which appeared while the present paper was going through the press, Professor E. H. Moore takes up my first (three-postulate) definition of a group,

$$(H_1) : (2', 9', 10'),$$

and after pointing out that the postulate $2'$ can be broken up into two component statements $2'_1$ and $2'_2$, raises the question as to the independence of the four postulates

$$(H'_1) : (2'_1, 2'_2, 9', 10').$$

As an answer to this question the following result may be not without interest: I find that either of the postulates $2'_1$ and $2'_2$ can be deduced as a theorem from the remaining three. That is, my first definition (H_1) may be replaced by a new three-postulate definition, say

$$(H''_1) : (2'_2, 9', 10'),$$

in which the postulate $2'_2$ is "milder" than the postulate $2'$. (The old proofs of independence hold for (H''_1), for both finite and infinite groups.)

The actual deduction of $2'_1$ from $9'$, $10'$ and $2'_2$ proceeds as follows:‡ We have

$9'$) *For every two elements* a, b *there is an element* x *such that* $a \circ x = b$.

$10'$) *For every two elements* a, b *there is an element* y *such that* $y \circ a = b$.

$2'_2$) *If* a, b, c *are three elements such that the products* $a \circ b$, $b \circ c$ *and* $a \circ (b \circ c)$ *belong to the set, then* $(a \circ b) \circ c = a \circ (b \circ c)$.

Lemma. *If* $a \circ b = a \circ b'$ *(both products belonging to the set), then* $b = b'$.

Proof. Let $c = a \circ b = a \circ b'$, and by $9'$ take x so that $b \circ x = b'$. Then, by hypothesis, $a \circ (b \circ x) = c$; or, by $2'_2$, $(a \circ b) \circ x = c$; or, $c \circ x = c$. Now by $10'$ take y so that $y \circ c = b$. Then $y \circ (c \circ x) = b$; or, by $2'_2$, $(y \circ c) \circ x = b$; or, $b \circ x = b$. Hence $b = b'$.

Theorem $2'_1$. *If* a, b, c *are three elements such that the products* $a \circ b$, $b \circ c$ *and* $(a \circ b) \circ c$ *belong to the set, then* $(a \circ b) \circ c = a \circ (b \circ c)$.

Proof. By $9'$ take x so that $a \circ x = (a \circ b) \circ c$ and also z so that $b \circ z = x$. Then $a \circ (b \circ z) = (a \circ b) \circ c$. But by $2'_2$, $a \circ (b \circ z) = (a \circ b) \circ z$. Therefore $c = z$, by the Lemma. Hence $b \circ c = x$; or, $a \circ (b \circ c) = (a \circ b) \circ c$.

In like manner we might have deduced $2'_2$ from $9'$, $10'$ and $2'_1$.

Harvard University,
October 31, 1902.

* Received for publication November 26, 1902.

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

‡ In the case of Abelian groups this deduction is not necessary.