POSTULATES FOR THE INVERSE OPERATIONS IN A GROUP*

BY

MORGAN WARD

1. **Introduction.** Suppose that we are given a collection of marks which we shall call "$\mathfrak{S}$-symbols," and a rule which assigns to any two $\mathfrak{S}$-symbols x and y a unique third $\mathfrak{S}$-symbol z. We may then regard z as a one-valued "function" of x and y defined over the collection $\mathfrak{S}$ and write

$$z = F(x, y). \tag{1}$$

It may happen that the function F is of such a character that when the $\mathfrak{S}$-symbols z, x are given in (1), an $\mathfrak{S}$-symbol y is uniquely determined, and when the $\mathfrak{S}$-symbols y, z are given in (1), an $\mathfrak{S}$-symbol x is uniquely determined. In this case we may associate with the function $F(x, y)$ two other one-valued functions $y=G(z, x)$, $x=H(y, z)$ defined over the collection $\mathfrak{S}$. These functions are called the first and second *inverses* of the function F. The primary object of this paper is to state the restrictions which must be imposed upon F in order that one of its inverses may define with $\mathfrak{S}$ an abstract group.

It is convenient, in developing the properties of the system $\{\mathfrak{S}; \circ\}$ consisting of the $\mathfrak{S}$-symbols, F, and one or more postulates, to replace (1) by the notation†

$$z = x \circ y.$$

In any interpretation of the $\mathfrak{S}$, we may look upon $\circ$ as an *operation* which we perform upon x and y to obtain z. We shall continue to call $\circ$ an operation even when no interpretation of the $\mathfrak{S}$-symbols is in mind, and we shall similarly replace $y=G(z, x)$ and $x=H(y, z)$ by

$$y = z\Delta x \quad \text{and} \quad x = y \square z.$$

For example, suppose that the $\mathfrak{S}$-symbols stand for the rational integers, and that $F(x, y)=x-y$. Then $z=x-y$; $y=-z+x$; $x=y+z$, so that $\circ$ is subtraction, $\square$, addition, and Δ, the negative of subtraction. Our problem in this instance would be first of all to frame a definition of "subtraction," and then to define "addition" in terms of "subtraction."

* Presented to the Society, April 5, 1930; received by the editors of the Bulletin in January, 1929, and transferred to the Transactions.

† Read "z equals x dot y."

2. **Postulates for the operation** $\circ$. Consider first the system $\{\mathfrak{S}; \circ\}$ consisting of (i) a collection $\mathfrak{S}$ of two or more distinct elements $a, b, c, \cdots$, (ii) a function $F(x, y) = x \circ y$ defined over $\mathfrak{S}$, and (iii) the following four postulates:

POSTULATE 1. *If a, b are any elements of $\mathfrak{S}$, then $a \circ b$ is an element of $\mathfrak{S}$ uniquely determined by a and b.*

POSTULATE 2. *If a, b are any elements of $\mathfrak{S}$, then $a \circ a = b \circ b$.*

POSTULATE 3. *If a, b, c are any elements of $\mathfrak{S}$, and 1 is the element of definition 1 below, $(a \circ b) \circ c = a \circ (c \circ (1 \circ b))$.*

POSTULATE 4. *If a, b are any elements of $\mathfrak{S}$, and 1 is the element of Definition 1 below, and if $1 \circ a = 1 \circ b$, then $a = b$.*

THEOREM 1. *There exists a unique element i of $\mathfrak{S}$ such that $i \circ i = i$.*

By Postulate 1, $a \circ a = i$ is an element of $\mathfrak{S}$, and by Postulate 2, $i \circ i = a \circ a = i$. Moreover, if j were any second element such that $j \circ j = j$, then by Postulate 2,

$$j = j \circ j = i \circ i = i.$$

DEFINITION 1. *The element i of Theorem 1 is called the "identity" of $\mathfrak{S}$ and denoted by 1, so that Theorem 1 states that for any element a of $\mathfrak{S}$*

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

Postulates 1, 3 and 4 are true in any Abelian group, or any Abelian semi-group containing an identity. Postulate 4 is in fact a weakened form of Dickson's third postulate for a semi-group.* Postulate 2 is far more drastic, and serves to give the system its peculiar character.

3. **Consistency and independence of postulates.** The consistency and independence of the four postulates given in §2 is proved by the following table, which gives examples of systems in which Postulates 1–4 are all true, Postulate 1 false and Postulates 2, 3, 4 true and so on.

It should be noted that in order to prove that Postulate 1 is independent, we must change the statement of the remaining postulates slightly. Thus Postulate 2 should read *If a, b are any two elements of $\mathfrak{S}$, and if $a \circ a$, $b \circ b$ are both in $\mathfrak{S}$, then $a \circ a = b \circ b$.* The similar emendations of Postulate 3 and Postulate 4 are left to the reader.

---

* L. E. Dickson, *On semi-groups and the general isomorphism between infinite groups*, these Transactions, vol. 6 (1905), p. 205. Also see Theorem 5, §4, Theorem 10, §6.

TABLE I

		$\mathfrak{S}$	$x \circ y$
	Consistency		
1.	All four true	Rational integers	$x-y$
2.	All four true	Rationals, 0 excluded	$x \div y$
	Independence		
3.	Postulate 1 false	Rational integers, 2 excluded	$x-y$
4.	Postulate 2 false	Rational integers	$x+y$
5.	Postulate 3 false	Rational integers	$y-x$
6.	Postulate 4 false	Rationals, 0 excluded	$\lvert x \rvert \div \lvert y \rvert$

4. **Deductions from postulates.** The five theorems which follow give important properties of the system $\{\mathfrak{S}; \circ\}$ defined in §2, and lead up to the fundamental theorem of the next section. The proofs of the theorems are given in some detail in order to bring out clearly the implications of the various postulates.

THEOREM 2. *If a is any element of $\mathfrak{S}$, then $a \circ 1 = a$.*

We have $1 \circ a = (1 \circ 1) \circ a = 1 \circ (a \circ (1 \circ 1)) = 1 \circ (a \circ 1)$ by Theorem 1 and Postulate 3. Therefore, by Postulate 4, $a = a \circ 1$.

THEOREM 3. *If a is any element of $\mathfrak{S}$, then $1 \circ (1 \circ a) = a$.*

We have $1 \circ a = (1 \circ a) \circ 1 = 1 \circ (1 \circ (1 \circ a))$, by Theorem 2 and Postulate 3. Therefore, by Postulate 4, $a = 1 \circ (1 \circ a)$.

THEOREM 4. *If a, b, c are any three elements of $\mathfrak{S}$, then $a \circ (b \circ c) = (a \circ (1 \circ c)) \circ b$.*

We have $a \circ (b \circ c) = a \circ [b \circ (1 \circ (1 \circ c))] = (a \circ (1 \circ c)) \circ b$, by Theorem 3 and Postulate 3.

THEOREM 4.1. *If a, b are any elements of $\mathfrak{S}$, then $1 \circ (a \circ b) = b \circ a$.*

We have $1 \circ (a \circ b) = (1 \circ (1 \circ b)) \circ a = b \circ a$ by Theorem 4 and Theorem 3.

THEOREM 5. *If a, b, c are any elements of $\mathfrak{S}$ and if* (i) $b \circ a = c \circ a$, *then $b = c$; and if* (ii) $a \circ b = a \circ c$, *then $b = c$.*

(i) is clear from Postulate 4, since by Theorem 4 and Postulate 2

$$(1 \circ a) \circ (b \circ a) = [(1 \circ a) \circ (1 \circ a)] \circ b = 1 \circ b;$$
$$(1 \circ a) \circ (c \circ a) = [(1 \circ a) \circ (1 \circ a)] \circ c = 1 \circ c.$$

(ii) follows from (i) and Theorem 4.1.

THEOREM 6. *If a, b, c are any three elements of $\mathfrak{S}$, the three relations*

$$a \circ b = c, \tag{2}$$

$$b = (1 \circ c) \circ (1 \circ a), \tag{3}$$

$$a = c \circ (1 \circ b) \tag{4}$$

are all equivalent to one another.

Note that in accordance with our definitions in §1, (3) and (4) give the first and second inverses of the operation $\circ$ in terms of $\circ$ itself.

(2) implies (3); for if $a \circ b = c$, then by Theorem 4.1,

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

Hence

$$(1 \circ c) \circ (1 \circ a) = (b \circ a) \circ (1 \circ a) = b \circ [(1 \circ a) \circ (1 \circ a)] = b \circ 1 = b,$$

by Postulate 3, Postulate 4 and Theorem 2. Conversely, (3) implies (2); for all the steps in the reasoning above are reversible.

(3) is equivalent to (4); for writing $(1 \circ c)$, $(1 \circ a)$, b for a, b, c in (2), we see from what we have just proved that (3) is equivalent to

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

Hence

$$1 \circ a = (1 \circ b) \circ c = 1 \circ (c \circ (1 \circ b))$$

by Theorem 3 and Postulate 3. Hence by Postulate 2, (3) is equivalent to (4), so that each of (2), (3) and (4) implies the other two.

5. **The operation $\square$.** We shall now study the second inverse of $\circ$ as defined by equation (4) of Theorem 6.

DEFINITION 2. *If x, y are any two elements of $\mathfrak{S}$,*

$$x \square y = y \circ (1 \circ x).$$

FUNDAMENTAL THEOREM. *$\mathfrak{S}$ forms a group with respect to the operation $\square$.*

(i) By Definition 2, Theorem 1 and Postulate 1, if a and b are any elements of $\mathfrak{S}$, $a \square b$ is an element of $\mathfrak{S}$ uniquely determined by a and b.

(ii) If a, b, c are any elements of $\mathfrak{S}$, then

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

For by Definition 2,

$$(a \square b) \square c = c \circ [1 \circ (b \circ (1 \circ a))];$$

$$a \square (b \square c) = [c \circ (1 \circ b)] \circ (1 \circ a).$$

Now

$$[c \circ (1 \circ b)] \circ (1 \circ a) = c \circ [(1 \circ a) \circ (1 \circ (1 \circ b))] = c \circ [(1 \circ a) \circ b],$$

by Postulate 3, Theorem 2. And by Theorem 4, Theorem 2,

$$c \circ [1 \circ (b \circ (1 \circ a))] = c \circ [(1 \circ (1 \circ (1 \circ a))) \circ b] = c \circ [(1 \circ a) \circ b].$$

(iii) The set contains an element i such that for any element a of the set, $i \square a = a \square i = a$.

For by Definition 2, Theorems 1, 2, 4, $\mathfrak{S}$ contains 1 and

$$1 \square a = a \circ (1 \circ 1) = a \circ 1 = a,$$
$$a \square 1 = 1 \circ (1 \circ a) = a,$$

so that we may take $i = 1$.

(iv) If a is any element of $\mathfrak{S}$, the set also contains an element a' such that $a \square a' = i$.

For by Definition 2, Postulate 2,

$$a \square (1 \circ a) = (1 \circ a) \circ (1 \circ a) = 1.$$

Hence we may take $a' = 1 \circ a$, and the system $\{\mathfrak{S}; \square\}$ satisfies the four postulates for a group.*

Consider the inverses of $\square$ in their relation to the original operation $\circ$.

THEOREM 7. *If* $b \square c = a$, *then* $c = (1 \circ b) \square a = a \circ b$, *and* $b = a \square (1 \circ c) = (1 \circ c) \circ (1 \circ a)$.

This is clear from Definition 2 and Theorem 6.

Thus the first inverse of $\square$ is $\circ$, while the second inverse of $\square$ is, by equation (3), the same as the first inverse of $\circ$.

6. **The operation Δ.** We shall now study the operation defined by equation (3).

DEFINITION 3. *If* x, y *are any two elements of* $\mathfrak{S}$,

$$x \Delta y = (1 \circ x) \circ (1 \circ y).$$

Since as we might expect, the operation Δ is very similar to the original operation $\circ$, we shall merely state its more important properties. The following four theorems which correspond roughly to Theorems 1 to 6 may all be proved from Definition 3 and the results already given.

THEOREM 8. (i) $a \Delta a = 1$; (ii) $a \Delta 1 = 1 \circ a$; (iii) $1 \Delta a = a$; (iv) $(a \Delta 1) \Delta 1 = a$; (v) $(a \Delta b) \Delta 1 = b \Delta a$; (vi) $1 \circ (a \Delta b) = b \Delta a$.

THEOREM 9. (i) $a \Delta (b \Delta c) = ((b \Delta 1) \Delta a) \Delta c$; (ii) $(a \Delta b) \Delta c = b \Delta ((a \Delta 1) \Delta c)$.

* Speiser, *Die Theorie der Gruppen*, Berlin, 1927, pp. 10–11.

THEOREM 10. *If* $a\Delta b = a\Delta c$, *then* $b=c$; *if* $b\Delta a = c\Delta a$, *then* $b=c$.

THEOREM 11. *If* $b = c\Delta a$, *then* $a \circ b = c$, *and* $b\square c = a$.

For example, Theorem 9 (ii) may be proved as follows.

By Definition 3, $(a\Delta b)\Delta c = [1 \circ (a\Delta b)] \circ (1 \circ c)$. Therefore,

$$(a\Delta b)\Delta c = [b\Delta a] \circ (1 \circ c) = [(1 \circ b) \circ (1 \circ a)] \circ (1 \circ c)$$
$$= (1 \circ b) \circ [(1 \circ c) \circ (1 \circ (1 \circ a))],$$

by Theorem 8 (vi), Definition 3, and Postulate 2. Hence by Theorem 3, Postulate 2, Definition 3,

$$(a\Delta b)\Delta c = (1 \circ b) \circ [(1 \circ c) \circ a] = (1 \circ b) \circ [1 \circ (a \circ (1 \circ c))];$$
$$(a\Delta b)\Delta c = b\Delta[a \circ (1 \circ c)].$$

Putting $b=1$ in this last result,

$$(a\Delta 1)\Delta c = 1\Delta[a \circ (1 \circ c)]$$
$$= a \circ (1 \circ c)$$

by Theorem 8 (iii). Hence

$$(a\Delta b)\Delta c = b\Delta((a\Delta 1)\Delta c).$$

7. **Postulates for the operation Δ.** It remains to give a set of postulates for the operation Δ which shall be consistent and independent.

THEOREM 12. *The system* $\{\mathfrak{S}; \Delta\}$ *satisfies the following four conditions*:

POSTULATE 1. *If* a, b *are any elements of* $\mathfrak{S}$, $a\Delta b$ *is an element of* $\mathfrak{S}$ *uniquely determined by* a *and* b.

POSTULATE 2. *If* a, b *are any elements of* $\mathfrak{S}$, $a\Delta a = b\Delta b$.

POSTULATE 5. *If* a, b, c *are any elements of* $\mathfrak{S}$, *and* 1 *is the element of Theorem* 1 *and Theorem* 8, $(a\Delta b)\Delta c = b\Delta((a\Delta 1)\Delta c)$.

POSTULATE 6. *If* a, b *are any elements of* $\mathfrak{S}$, *and* 1 *is the element of Theorem* 1 *and Theorem* 8, *and if* $a\Delta 1 = b\Delta 1$, *then* $a=b$.

The proof is clear from Theorems 8–11.

Table I of §3 may easily be modified so as to show that these postulates are consistent and independent.

8. **Condition that $\square$ be commutative.** We shall now give a condition that the operation $\square$ be commutative, so that $\{\mathfrak{S}; \square\}$ will form an Abelian group.

THEOREM 13. *A necessary and sufficient condition that the operation* $\square$ *of Definition* 2 *be commutative is that, for every pair of elements* a, b *of* $\mathfrak{S}$, $a\Delta b = b \circ a$.

The condition is necessary; for if $\square$ is commutative, and if a, b are any two elements of $\mathfrak{S}$, then

$$a \square b = b \square a. \tag{5}$$

Then by Definition 2,

$$b \circ [b \circ (1 \circ a)] = b \circ [a \square b] = b \circ [b \square a] = b \circ [a \circ (1 \circ b)].$$

But

$$b \circ [b \circ (1 \circ a)] = (b \circ a) \circ b; \quad b \circ [a \circ (1 \circ b)] = 1 \circ a,$$

by Theorem 4, Theorem 3 and Theorem 1. Hence (5) implies that

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

By Theorem 6 and Definition 3, this last equation is equivalent to

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

The condition is moreover sufficient, for all the steps in the reasoning just given are reversible.

We close with a table giving the relations between the various operations and their inverses.

TABLE II

Operation	First Inverse	Second Inverse
$z = x \circ y$	$y = z \Delta x$	$x = y \square z$
$x = y \square z$	$z = x \circ y$	$y = z \Delta x$
$y = z \Delta x$	$x = y \square z$	$z = x \circ y$

I wish to express my thanks to the editors of this journal for some extremely helpful criticisms and suggestions.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.