THE INVERSE OPERATION IN GROUPS

HARRY FURSTENBERG

1. **Introduction.** In the theory of groups, the product ab^{-1} occurs frequently in connection with the definition of subgroups and cosets. This suggests that the entire theory of groups might have been presented using the inverse operation ab^{-1}, rather than ab. A neat formulation of the group postulates in terms of the inverse operation for arbitrary groups is not obvious, and thus the system of postulates (for non-abelian groups) proposed, for example, by [1], actually first defines addition in terms of subtraction and restates the group axioms (in particular, associativity) in terms of subtraction. The object of this paper is to present a system of postulates for the inverse operation which is actually more concise than the usual formulation in terms of ordinary multiplication. We shall also study systems which are suggested by these axioms in the same way as semigroups are derived from the group axioms. It turns out that while very little can be said about an arbitrary semigroup, it is possible to determine completely the structure of the analogous system which we call a "half-group."

2. **The group postulates.** We consider a system G in which an operation $a \circ b$ is defined satisfying the following set of postulates:

(1) $a \circ b \in G$ for any $a, b \in G$.

(2) $(a \circ c) \circ (b \circ c) = a \circ b$ for any $a, b, c \in G$.

(3) $a \circ G = G$ for any $a \in G$.

We note, first of all, that in a system satisfying (1) and (2), (3) implies the following two axioms:

(3a) There exists an $e \in G$ satisfying $a \circ a = e$ for all $a \in G$.

(3b) $a \circ e = a$.

To show this, let $e = a \circ a$ for some a. By (3), $x = a \circ x'$ for any x and some appropriate x', so that $x \circ x = (a \circ x') \circ (a \circ x') = a \circ a = e$ by (2). Moreover $x \circ e = (a \circ x') \circ (x' \circ x') = a \circ x' = x$ which proves (3b). We can now prove the following theorem:

THEOREM 1. *Any system G satisfying* (1), (2), *and* (3) *is a group*

Received by the editors January 18, 1955.

under the operation $ab = a \circ (e \circ b)$, *and for multiplication defined in this way,* $a \circ b = ab^{-1}$.

PROOF. We may assume that G satisfies (1), (2), (3a), (3b). We notice first of all that $e \circ (e \circ a) = (a \circ a) \circ (e \circ a) = a \circ e = a$. Therefore e acts as the identity, for, $ae = a \circ (e \circ e) = a \circ e = a$, and $ea = e \circ (e \circ a) = a$. Define $a^{-1} = e \circ a$. Then $aa^{-1} = a(e \circ a) = a \circ [e \circ (e \circ a)] = a \circ a = e$, and $a^{-1}a = (e \circ a) \circ (e \circ a) = e$. It is now necessary only to prove associativity for this system. To do this we consider the product $[a \circ (e \circ b)] \circ \{[e \circ (b \circ c^{-1})] \circ [(e \circ c^{-1}) \circ (b \circ c^{-1})]\}$. This equals, on the one hand, $[a \circ (e \circ b)] \circ [e \circ (e \circ c^{-1})] = [a \circ (e \circ b)] \circ c^{-1} = (ab) \circ (e \circ c) = (ab)c$. It also equals $[a \circ (e \circ b)] \circ \{[e \circ (b \circ c^{-1})] \circ (e \circ b)\} = a \circ [e \circ (b \circ c^{-1})] = a(b \circ c^{-1}) = a(b \circ (e \circ c)) = a(bc)$ which establishes associativity. It is clear that $ab^{-1} = a \circ (e \circ b^{-1}) = a \circ [e \circ (e \circ b)] = a \circ b$ which completes the proof.

We observe that the assumptions of closure, associativity, and the solvability of $ax = b$ in a system, which correspond to our postulates (1), (2), and (3), do not suffice to make it a group. This lies in the strength of postulate (2) as we shall see later. We first state

THEOREM 2. *Let G be a group satisfying, in addition:*

(4) $(c \circ b) \circ (c \circ a) = a \circ b$ *for all* $a, b, c \in G$; *then G is abelian.*

PROOF. This is clear since $ab = a \circ (e \circ b) = [e \circ (e \circ b)] \circ (e \circ a) = b \circ (e \circ a) = ba$. We note in passing that (4) together with (2) imply (3a), for $a \circ a = (a \circ b) \circ (a \circ b) = b \circ b$. We require for later use the fact that if G satisfies (1), (2), and (3) it is a group and therefore also satisfies $G \circ a = G$.

THEOREM 3. *Let G satisfy* (1), (2), *and* (3a). *If furthermore $G \circ G = G$, that is, every element of G is a product, then G is a group.*

PROOF. We shall prove (3b) holds in such a system. Any $x \in G$ can be written

$$x = x_1 \circ x_2 = (x_1 \circ x_2) \circ (x_2 \circ x_2) = x \circ e$$

which proves the theorem.

3. **The half-group.** A half-group is defined as a system G obeying (1) and (2). The object of the remainder of this paper will be to determine the structure of such a system. Our first problem is to show that the notions of cosets and factor groups can be extended to arbitrary half-groups. An element x is said to be "idempotent" if $x \circ x = x$. Any element of the form $a \circ a$ is idempotent since $(a \circ a) \circ (a \circ a) = a \circ a$. A "sub-half-group" $S \subset G$ is a subset closed under $a \circ b$ and which

contains all the idempotent elements of G. An "invariant" sub-half-group is one satisfying $a \circ (a \circ S) \subset S$ for all $a \in G$. We can define cosets with respect to any sub-half-group S by using the congruence relation: $a \equiv b$ if $a \circ b \in S$. We shall show that this is actually an equivalence relation:

(a) $a \equiv a$ since $a \circ a \in S$.

(b) $a \equiv b$ implies $b \equiv a$ since $b \circ a = (b \circ b) \circ (a \circ b) \in S$.

(c) $a \equiv b$ and $b \equiv c$ imply $a \circ b \in S$ and $c \circ b \in S$ whence $(a \circ b) \circ (c \circ b) \in S$ and $a \circ c \in S$ and $a \equiv c$.

If S is invariant in G, then we can define a multiplication of the cosets as $a^* \circ b^* = (a \circ b)^*$ (where x^* represents the coset to which x belongs). It is necessary to show that if $a \equiv a'$, $b \equiv b'$ then $(a \circ b) \equiv (a' \circ b')$. Now $a' \circ a \in S$ implies $(a' \circ b) \circ (a \circ b) \in S$ or $a' \circ b \equiv a \circ b$. Also $b' \circ b \in S$ implies $(a' \circ b) \circ [(a' \circ b) \circ (b' \circ b)] \in S$ by the invariance of S, whence $(a' \circ b) \circ (a' \circ b') \in S$ and $a' \circ b \equiv a' \circ b'$. We therefore have $a \circ b \equiv a' \circ b'$. The set of cosets then has an operation $a^* \circ b^*$ defined on it and we may speak of the system $\{G/S, \circ\}$.

THEOREM 4. *G/S is a half-group satisfying* (3a).

PROOF. (1) is obviously true for G/S. Also $(a^* \circ c^*) \circ (b^* \circ c^*) = (a \circ c)^* \circ (b \circ c)^* = [(a \circ c) \circ (b \circ c)]^* = (a \circ b)^* = a^* \circ b^*$ which proves (2). Moreover $a^* \circ a^* = (a \circ a)^*$ which is the unique coset containing S. This proves the theorem. It might be mentioned that if $G \circ G = G$ then G/S is a group as follows from Theorem 3.

4. **Equivalent extensions and retractions.** We now define an equivalence relation ($\sim$) in a half-group, G. Let $a \sim b$ if there exists an $x \in G$ such that $a \circ x = b \circ x$.

THEOREM 5. *$a \sim b$ implies $a \circ y = b \circ y$ and $y \circ a = y \circ b$ for all $y \in G$.*

PROOF. $a \circ y = (a \circ x) \circ (y \circ x) = (b \circ x) \circ (y \circ x) = b \circ y$; $y \circ a = (y \circ y) \circ (a \circ y) = (y \circ y) \circ (b \circ y) = y \circ b$. Q.E.D.

THEOREM 6. *$a \sim b$ is an equivalence relation.*

PROOF. Reflexitivity and symmetry are obvious. Also $a \sim b$ and $b \sim c$ imply $a \circ x = b \circ x = c \circ x$ by Theorem 5 so that $a \sim c$. Q.E.D.

THEOREM 7. *$a \sim b$ and $a_1 \sim b_1$ imply $a \circ a_1 = b \circ b_1$.*

PROOF. $a \circ y_1 = b \circ a_1 = b \circ b_1$ by Theorem 5. Q.E.D.

It is clear that given a half-group G, we can obtain a larger half-group $\overline{G}$ by arbitrarily adjoining elements to G and assigning to each $\bar{x} \in \overline{G} - G$ an element $x \in G$ and agreeing that $\bar{x}$ multiplied by any

member of G should yield the same result as x multiplied by that element. (The product $\bar{x} \circ \bar{y}$ for both $\bar{x}, \bar{y} \in \overline{G} - G$ would also be defined as $\bar{x} \circ \bar{y} = x \circ y$.) If (2) held for G it must still hold for $\overline{G}$. In other words, if $\overline{G}$ is obtained from G by arbitrarily adjoining "equivalent" elements, then $\overline{G}$ is still a half-group. We shall call $\overline{G}$ an "equivalent extension" of G. In a similar manner we obtain an "equivalent retraction" of G by identifying equivalent elements of G and denoting them by one element. More precisely, $\tilde{G}$ is an equivalent retraction of G if there exists a single-valued function f from G onto $\tilde{G}$, preserving multiplication and such that $f(x) = f(y)$ only if $x \sim y$. It is clear that if G is a half-group then $\tilde{G}$ is also one. For $[f(a) \circ f(c)] \circ [f(b) \circ f(c)] = [f(a \circ c)] \circ [f(b \circ c)] = f[(a \circ c) \circ (b \circ c)] = f(a \circ b) = f(a) \circ f(b)$.

THEOREM 8. *Every half-group G is the equivalent extension of a sub-half group G' for which $G' \circ G' = G'$.*

PROOF. Let $G' = G \circ G$. G' is a sub-half-group since it is closed under multiplication and contains the idempotent elements. $x \in G'$ implies $x = x_1 \circ x_2$ for $x_1, x_2 \in G$ or $x = (x_1 \circ r) \circ (x_2 \circ r)$ for an arbitrary r so that $x \in G' \circ G'$ whence $G' = G' \circ G'$. Now let $x \in G$ and a be any element of G'. Then $a = a_1 \circ a_2$ so that $x \circ a = x \circ (a_1 \circ a_2) = [x \circ (a_2 \circ a_2)] \circ [(a_1 \circ a_2) \circ (a_2 \circ a_2)] = [x \circ (a_2 \circ a_2)] \circ (a_1 \circ a_2)$ whence $x \sim x \circ (a_2 \circ a_2) \in G'$ which proves the theorem. As a result of Theorem 8 it is necessary for us to consider only half-groups G such that $G \circ G = G$, since any other half-group is an equivalent extension of one such. In our further discussion we shall assume, then, that $G \circ G = G$.

Given two half-groups G_1 and G_2, there is no difficulty in defining their "direct product" $G_1 \times G_2$. It is, in fact, the set of all pairs (g_1, g_2) with $g_1 \in G_1$, and $g_2 \in G_2$. $(g_1, g_2) \circ (g_1' \circ g_2') = (g_1 \circ g_1', g_2 \circ g_2')$.

We now give an example of a half-group which is not in general a group. Consider the set of all pairs (m, n) where m and n belong to a fixed set M. Define $(m_1, n_1) \circ (m_2, n_2) = (m_1, m_2)$. We have $[(m_1, n_1) \circ (m_3, n_3)] \circ [(m_2, n_2) \circ (m_3, n_3)] = (m_1, m_3) \circ (m_2, m_3) = (m_1, m_2) = (m_1, n_1) \circ (m_2, n_2)$. We call such a half-group a "simple" half-group. Our main result which we shall demonstrate in the next section states that any half-group can be derived from the direct product of a group with a simple half-group by taking equivalent extensions and retractions.

5. **The structure theorem for half-groups.** Define I as the set of all elements equivalent to idempotent elements. (We assume $G = G \circ G$.) To prove that I is a sub-half-group we observe first that if e_1 and e_2

are idempotent then $e_1 \circ e_2 \sim e_1$. For $e_1 \circ e_2 = (e_1 \circ e_2) \circ (e_2 \circ e_2) = (e_1 \circ e_2) \circ e_2$ so that $e_1 \sim e_1 \circ e_2$. Now $x_1 \sim e_1$ and $x_2 \sim e_2$ imply $x_1 \circ x_2 = e_1 \circ e_2$ by Theorem 7 and $x_1 \circ x_2 \sim e_1$ so that $x_1 \in I$ and $x_2 \in I$ imply $x_1 \circ x_2 \in I$. The idempotent elements belong to I so that I is a sub-half-group. We observe that $x = a \circ e$ with e idempotent implies $x \circ e = (a \circ e) \circ (e \circ e) = a \circ e$ whence $x \sim a$ so that if $y \in I$ then $y \sim e$ with e idempotent, and $z \circ y = z \circ e \sim z$, $z \circ [z \circ y] = z \circ z \in I$ and finally $z \circ [z \circ I] \subset I$. I is therefore an invariant sub-half-group of G and G/I is a group by Theorems 3 and 4. Let $(\equiv)$ denote congruence mod I. We can then state

THEOREM 9. (a) *$a \equiv b$ implies $x \circ a \sim x \circ b$.*

(b) *The congruences $a \circ x \equiv b$ and $x \circ a \equiv b$ each have one and only one solution except for congruences.*

(c) *$e_1 \circ (e_2 \circ x) \equiv x$ for $e_1, e_2 \in I$.*

(d) *$e_1 \circ y_1 = e_2 \circ y_2$ implies $e_1 = e_2$ if e_1 and e_2 are idempotent.*

PROOF. (a) $a \circ b \in I$ implies $a \circ b \sim e'$ with e' idempotent. Now $x \circ a = (x \circ b) \circ (a \circ b) = (x \circ b) \circ e' \sim (x \circ b)$. (b) and (c) both follow immediately by passing over to the group G/I and replacing the congruences by equations involving cosets. In (d) we also observe by passing over to G/I that $y_1 \equiv y_2$ whence $e_1 \circ y_1 \sim e_1 \circ y_2$ by (a). Since $e_2 \circ y_2 = e_1 \circ y_1$ we have $e_2 \circ y_2 \sim e_1 \circ y_2$ and $(e_2 \circ y_2) \circ (y_2 \circ y_2) = (e_1 \circ y_2) \circ (y_2 \circ y_2)$ or $e_2 \circ y_2 = e_1 \circ y_2$ and $e_2 \sim e_1$. Therefore $e_2 = e_2 \circ e_2 = e_2 \circ e_1 = e_1 \circ e_1 = e_1$.

Define E as the simple half-group obtained from the set of idempotent elements of G. In other words E is the set of all pairs of idempotent elements, (e', e''). We know that any half-group is derived from one satisfying $G \circ G = G$ by an equivalent extension. We now prove for a G satisfying $G \circ G = G$

THEOREM 10. *G is an equivalent retraction of the direct product of the group G/I with the simple half-group E.*

PROOF. We denote the elements of $G/I \times E$ by (t, e', e'') with $t \in G/I$ and $(e', e'') \in E$. Multiplication is defined by $(t_1, e_1', e'') \circ (t_2, e_2', e_2'') = (t_1 \circ t_2, e_1', e_2')$ using the rule for multiplication in simple half-groups. We shall define a function from $G/I \times E$ to G which we shall show determines an equivalent retraction. For any $(t, e', e'') \in G/I \times E$, let $a^* = t$; the equations $e' \circ x \equiv a$, $e'' \circ y \equiv x$ have solutions unique up to congruences, by Theorem 9(b). Define $f(t, e', e'') = e' \circ (e'' \circ y)$. If x_1, y_1 is another solution to the above equations, then $y_1 \equiv y$ and $e'' \circ y_1 \sim e'' \circ y$, $e' \circ [e'' \circ y_1] = e' \circ [e'' \circ y]$ so that f is single-valued.

Let $\lambda \in G$. Then $\lambda = \lambda_1 \circ \lambda_2$. We shall see that $f(\lambda^*, \lambda_1 \circ \lambda_1, \lambda_2 \circ \lambda_2) = \lambda$. For, a solution to the congruence $e' \circ x \equiv \lambda$ or $(\lambda_1 \circ \lambda_1) \circ x \equiv \lambda_1 \circ \lambda_2$ is $x = \lambda_2 \circ \lambda_1$. A solution of $e'' \circ y \equiv \lambda_2 \circ \lambda_1$ or $(\lambda_2 \circ \lambda_2) \circ y = \lambda \circ \lambda_1$ is $y = \lambda_1 \circ \lambda_2$ whence $f(\lambda^*, \lambda_1 \circ \lambda_1, \lambda_2 \circ \lambda_2) = (\lambda_1 \circ \lambda_1) \circ [(\lambda_2 \circ \lambda_2) \circ (\lambda_1 \circ \lambda_2)] = (\lambda_1 \circ \lambda_1) \circ (\lambda_2 \circ \lambda_1) = \lambda_1 \circ \lambda_2 = \lambda$. f is therefore "onto."

We must show that $f(\alpha) = f(\beta)$ implies $\alpha \sim \beta$. We notice that since the rule for the multiplication of (t, e', e'') does not depend on e'', $(t, e', e_1'') \sim (t, e', e_2'')$. $f(t_1, e_1', e_1'') = f(t_2, e_2', e_2'')$ implies $e_1 \circ (e_1'' \circ y_1) = e_2' \circ (e_2'' \circ y_2)$ and $e_1' = e_2'$ by Theorem 9(d). Moreover $a_1 \equiv e_1' \circ (e_1'' \circ y_1) = e_2' \circ (e_2'' \circ y_2) \equiv a_2$. Here y_1, y_2, a_1, a_2 are used as in the definition of f. Since $a_1 \equiv a_2$ we must have $t_1 = t_2$. Hence $(t_1, e_1', e_1'') \sim (t_2, e_2', e_2'')$ as was to be shown. It remains to prove that f preserves multiplication.

Let

$$f(t, e', e'') = e' \circ (e'' \circ y); \qquad e'' \circ y \equiv x, \qquad e' \circ x \equiv a, \qquad a^* = t.$$

$$f(t_1, e_1', e_1'') = e_1' \circ (e_1'' \circ y_1); \quad e_1'' \circ y_1 \equiv x_1, \quad e_1' \circ x_1 \equiv a_1, \quad a_1^* = t_1.$$

Then

$$f(t \circ t_1, e', e_1') = e' \circ (e_1' \circ y_2); e_1' \circ y_2 \equiv x_2, e' \circ x_2 \equiv a_2, a_2 \equiv a \circ a_1.$$

Now $(e' \circ a_1) \circ (a \circ a_1) = e' \circ a$. By Theorem 9(c), $e' \circ a_1 \equiv x_1$, $e' \circ a \equiv x$, $y_2 \equiv a_2$. We therefore obtain $x_1 \circ a_2 \equiv x$; $(e_1'' \circ y_1) \circ y_2 \equiv e'' \circ y$. By Theorem 9(a),

$$(e_1' \circ y_2) \circ [e_1'' \circ y_1) \circ y_2] \sim (e_1' \circ y_2) \circ (e'' \circ y)$$

or

$$e_1' \circ (e_1'' \circ y_1) \sim (e_1' \circ y_2) \circ (e'' \circ y)$$

whence

$$[e' \circ (e'' \circ y)] \circ [e_1' \circ (e_1'' \circ y_1)] = [e' \circ (e'' \circ y)] \circ [(e_1' \circ y_2) \circ (e'' \circ y)]$$

and

$$[e' \circ (e'' \circ y)] \circ [e_1' \circ (e_1'' \circ y_1)] = e' \circ (e_1' \circ y_2);$$

$$f(t, e', e'') \circ f(t_1, e_1', e_1'') = f(t \circ t_1, e', e_1') = f[(t, e', e'') \circ (t_1, e_1', e_1'')]$$

as was to be shown. This completes the proof.

For completeness we state:

THEOREM 11. *Every element of I is of the form $e' \circ e''$ where e' and e'' are idempotent.*

PROOF. Let $x \in I$. Then $x = x_1 \circ x_2 = (x_1 \circ x_2) \circ (x_2 \circ x_2) = x \circ (x_2 \circ x_2)$. Also $x \sim e'$ with e' idempotent, so that $x = e' \circ (x_2 \circ x_2) = e' \circ e''$ since $x_2 \circ x_2$ is idempotent. This shows, by the way, that every sub-half-group of G contains I.

We conclude with another example of a half-group that is not a group. Let G be the set of real numbers with $a \circ b$ defined as that x, $0 \leqq x < 1$ such that $a - b \equiv x \pmod 1$. It can be shown that G is a half-group, and is, in fact, an equivalent extension of the group R/Z —that is, the group of reals modulo 1.

REFERENCE

1. D. G. Rabinow, *Independent set of postulates for abelian groups and fields in terms of inverse operations*, Amer. J. Math. vol. 59 (1937) p. 211.

YESHIVA UNIVERSITY