Jour. Pure Math.
Vol. I (1981), pp. 73-75

CHARACTERIZATION OF GROUPS

M. K. Sen

In this short note we shall give a characterization of groups in terms of two binary operations.

Let G be a set with two binary operations $*$ and o, satisfying the following two axioms :

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

(2) $a \circ (b * a) = b$.

Lemma 1. If $a \circ a = a$ and $b \circ b = b$ in G, then $a = b$.

Proof.

$$b * a = (b \circ b) * a$$
$$= b \circ (a * b) \quad \text{by (1)}$$
$$= a. \quad \text{by (2)}$$

Hence $a = a \circ a = a \circ (b * a) = b$.

Lemma 2. If $e_a = a * a$, then $a \circ e_a = a$.

Proof. $a \circ (a * a) = a$. by (1)

Hence $a \circ e_a = a$.

Lemma 3. If $e_a = a * a$, then $e_a \circ e_a = e_a$

Proof. $a = a \circ (a * a)$. by (2)

$$a * a = (a \circ (a * a)) * a$$
$$= (a * a) \circ (a * a). \quad \text{by (1)}$$

This shows that $e_a \circ e_a = e_a$.

Lemma 4. e_a is independent of a, that is, $e_a = b * b$ for every b in G.

Proof. Let $e_b = b * b$. As in Lemma 3, we can show that $e_b \circ e_b = e_b$. Also we have $e_a \circ e_a = e_a$. Then from Lemma 1, it follows that $e_a = e_b$.

Let us write e for e_a.

Lemma 5. $e * b = b$ for all $b \in G$.

Proof.

$$e * b = (e \circ e) * b$$
$$= e \circ (b * e) \quad \text{by (1)}$$
$$= b. \quad \text{by (2)}$$

Lemma 6. $b \circ e = b$ for all $b \in G$.

Proof. $b \circ e = b \circ (b * b)$ by Lemma 4

$= b.$ by (2)

Lemma 7. $b * e = e \circ b$ for all $b \in G$.

Proof. $b * e = (b \circ e) * e$ by Lemma 6

$= e \circ (e * b)$ by (1)

$= e \circ b.$ by Lemma 5

Lemma 8. $a * (b \circ c) = (a * b) \circ c$ for all $a, b, c \in G$.

Proof. $a * (b \circ c) = (a \circ e) * (b \circ c)$ by Lemma 6

$= e \circ ((b \circ c) * a)$ by (1)

$= e \circ (c \circ (a * b))$ by (1)

$= (c \circ (a * b)) * e$ by Lemma 7

$= (a * b) \circ (e * c)$ by (1)

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

Theorem. If a binary operation in G is defined by $ab = (e \circ a) * b$ for all $a, b \in G$, then G is a group.

Proof. Let $a, b, c \in G$.

(1) Associativity :

$(ab)c = (e \circ ((e \circ a) * b)) * c$ by Definition

$= ((b \circ e) * (e \circ a)) * c$ by (1)

$= (b * (e \circ a)) * c$ by Lemma 6

$= ((b * e) \circ a) * c$ by Lemma 8

$= a \circ (c * (b * e))$ by (1)

$= a \circ (c * (e \circ b))$ by Lemma 7

$= a \circ ((c \circ e) * (e \circ b))$ by Lemma 8

$= a \circ (e \circ ((e \circ b) * c))$ by (1)

$= a \circ (((e \circ b) * c) * e)$ by Lemma 7

$= (e \circ a) * ((e \circ b) * c)$ by (1)

$= a(bc).$ by Definition

(2) Left identity :

$$\begin{aligned} eb &= (e \circ e) * b && \text{by Definition} \\ &= e \circ (b * e) && \text{by (1)} \\ &= b. && \text{by (2)} \end{aligned}$$

(3) Left inverse :

$$\begin{aligned} (e \circ a)a &= (e \circ (e \circ a)) * a && \text{by Definition} \\ &= ((e \circ a) * e) * a && \text{by Lemma 7} \\ &= (a \circ (e * e)) * a && \text{by (1)} \\ &= (a \circ e) * a && \text{by Lemma 5} \\ &= a * a && \text{by Lemma 6} \\ &= e. && \text{by Lemma 4} \end{aligned}$$

Hence G is a group.

Note 1. With respect to the operation $ab=(e \circ a) * b$ for all $a, b \in G$, G is a commutative group if $a * b = b \circ a$ for all $a, b \in G$.

Proof. Suppose $a * b = b \circ a$.

$$\begin{aligned} \text{Then } ab &= (e \circ a) * b && \text{by Definition} \\ &= b \circ (e \circ a) && \text{by Assumption} \\ &= b \circ (a * e) && \text{by Lemma 7} \\ &= (e \circ b) * a && \text{by (1)} \\ &= ba. \end{aligned}$$

Note 2. Let G be a group. If we define $a * b = a^{-1}b$ and $a \circ b = ab^{-1}$, then G satisfies both (1) and (2).

Received
10.9.81

Dept. of Pure Math.
Calcutta University