

A NOTE ON EQUIVALENT DEFINITIONS OF A GROUP

Dr. T. N. KAVITHA*

Assistant Professor of Mathematics,
 SCSVMV University, Enathur, Kanchipuram, India.

E. MANIVANNAN

M.Phil., Research scholar,
 SCSVMV University, Enathur, Kanchipuram, India.

(Received On: 13-02-17; Revised & Accepted On: 04-04-17)

ABSTRACT

The equivalent definition actually specifies a constant to be called the identity element (neutral element), and a unary operation that plays the role of the inverse map. To show the equivalence, we really need to show that the identity element and inverse map of a group are already uniquely determined by the binary operation.

1. INTRODUCTION

In mathematics, a **group** is an algebraic structure consisting of a set of elements equipped with an operation that combines any two elements to form a third element. The operation satisfies four conditions called the group axioms, namely closure, associativity, identity and invertibility.

The main difference is that the above definition (textbook definition) only postulates *existence* of an identity element (neutral element) and inverses, but does not include them as part of the group structure.

1.1 Definition: Let $*$ be a binary operation defined on G . an element $e \in G$ is called a left identity if $e * a = a$ for all $a \in G$. Then e is called a right identity if $a * e = a$ for all $a \in G$.

1.2 Example

1. In C we define $z \circ z = |z| \cdot z$. Here all elements z such that $|z| = 1$ are left identities.
2. In R we define $a * b = ab^2$. Here 1 and -1 are right identities.
3. In N we define $a * b = a$. Here every element is a right identity.

1.3 Definition: Let $*$ be a binary operation defined on G . Let $e \in G$ be the identity element. Let $a \in G$. An element $a' \in G$ is called a left inverse of a if $a' * a = e$. a' is called a right inverse of a if $a * a' = e$.

1.4 Note: The identity element e of a group G is both a left identity and a right identity. The inverse of any element $a \in G$ is both a left inverse and a right inverse.

1.5 Theorem: Let G be a non empty set with an associative binary operation defined on it such that there exists a left identity e in G and each element $a \in G$ has a left inverse a' with respect to e . Then G is a group.

Proof:

a' is a left inverse of a so that $a'a = e$.

let a'' be a left inverse of a' so that $a''a' = e$

then $aa' = e(aa')$ [since e is left identity]
 $= (a''a')(aa')$
 $= a''(a'a)$ [associative]
 $= a''(ea')$
 $= a''a'$ [since e is left identity]
 $= e$.

*Corresponding Author: Dr. T. N. Kavitha**

Hence, a' is also a right inverse of a .

Also, $a = ea = (aa')a = a(a'a) = ae$.

Hence, e is also a right identity.

Thus $ea = a = ae$ and $a'a = aa' = e$ and for all $a \in G$. Hence G is a group.

1.6 Theorem: Let G be a non empty set with an associative binary operation defined on it such that there exists a right identity e in G and each element $a \in G$ has a right inverse a' with respect to e . Then G is a group.

The proof is Similar to previous theorem.

1.7 Note: If G is a non empty set with an associative binary operation $*$ defined on it such that there exists a left identity and a right inverse for each element, then $(G, *)$ need not be a group.

For example, consider $(\mathbb{R}, *)$ where $a * b = |a|b$.

Clearly $*$ is a binary operation on \mathbb{R}^* .

Now, $a * (b * c) = (a * b) * c = |a||b|c$ and hence $*$ is associative.

$(-1) * a = |-1|a = a$

Hence -1 is a left identity.

Now, when $a < 0$;

$a * (1/a) = |a|(1/a) = (-a)(1/a) = -1$ and

when $a > 0$;

$a * (-1/a) = |a|(-1/a) = (a)(-1/a) = -1$.

Hence if $a < 0$, $(1/a)$ is the right inverse of a and if $a > 0$, $(-1/a)$ is the right inverse of a . However $(\mathbb{R}^*, *)$ is not a group since the equation $y * a = a$ has two solutions namely 1 and -1 .

1.8 Theorem: Let G be a non empty set with an associative binary operation defined on it such that the equation $ax = b$ and $ya = b$ have unique solutions for x and y in G . Then G is a group.

Proof:

Let $a \in G$. Then there exists a unique $e \in G$ such that $ea = a$.

Now, let b be any other element in G . then there exists a unique x in G such that $ax = b$

Now, $eb = e(ax) = (ea)x = ax = b$

$eb = b$ for all $b \in G$ so that e is a left identity.

Let $a \in G$. Then $ya = a$ has a unique solution a' .

$a'a = e$ so that a' is the left inverse of a .

Hence by theorem 4.1.5, G is a group.

1.9 Theorem: Let G be a finite set with an associative binary operation defined on G in which both cancellation laws hold good. Then G is a group.

Proof:

Let $G = \{ a_1, a_2, \dots, a_n \}$

Now let $a, b \in G$

Consider the elements aa_1, aa_2, \dots, aa_n .

All these elements are distinct, for if $aa_r = aa_s$ then $a_r = a_s$ (by cancellation law).

Hence aa_1, aa_2, \dots, aa_n are just the elements a_1, a_2, \dots, a_n of G in some order and hence $aa_i = b$ for some i .

Thus the equation $ax = b$ has a unique solution for x in G . Similarly taking the elements aa_1, aa_2, \dots, aa_n we can prove that the equation $ya = b$ has a unique solution for y in G .

Hence by previous theorem, G is a group.

1.10 Note: The above theorem is not true if G is infinite. For example, consider $(\mathbb{N}, +)$. Clearly $+$ is an associative binary operation defined on \mathbb{N} and both cancellation laws hold good in \mathbb{N} .

But $(\mathbb{N}, +)$ is not a group.

REFERENCE

- Clifford, A. H.; Preston, G. B. (1967), The Algebraic Theory of Semigroups, 2, American Mathematical Society, ISBN 978-0-8218-0272-4, Zbl 0178.01203.
- Grillet, Pierre A. (1995), Semigroups: An Introduction to the Structure Theory, Marcel Dekker, ISBN 978-0-8247-9662-4, Zbl 0830.20079.
- Grillet, Pierre A. (2001), Commutative Semigroups, Springer Verlag, ISBN 978-0-7923-7067-3, Zbl 1040.20048.
- Hollings, Christopher (2014), Mathematics across the Iron Curtain: A History of the Algebraic Theory of Semigroups, American Mathematical Society, ISBN 978-1-4704-1493-1, Zbl 06329297.

Source of support: Nil, Conflict of interest: None Declared.

[Copy right © 2017. This is an Open Access article distributed under the terms of the International Journal of Mathematical Archive (IJMA), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.]