Another definition of a group by means of a single axiom

by José Morgado

Instituto de Física e Matemática, Universidade Federal de Pernambuco, Brasil

Introduction

In [1], MICHAEL SLATER characterizes a group by means of a single axiom of the form p *implies* q, p and q being equations, in terms of two operations: a binary operation $\cdot$ (multiplication) and a unary operation $'$ (inversion). He proves that the system $< G, \cdot, ' >$ is a group, if and only if

$$ab \cdot c = ad \cdot e \text{ implies } b = d \cdot ec' .$$

In [2], p. 6, MARSHALL HALL gives a definition of a group in terms of one of the inverse operations of the multiplication by using four axioms.

In [3], it is observed that these axioms are not independent and one defines a group in terms of the same operation by using two axioms.

In [4], one obtains a definition of a group in terms of the same operation by means of one axiom of the form p *implies* q, where p and q are equations. It is shown that, if the groupoid $< G, \cdot >$ satisfies the condition

$$a(bb \cdot b) \cdot (cc \cdot c) = a(dd \cdot d) \cdot (ee \cdot e) \text{ implies } b = d \cdot ce ,$$

then, if one defines the operation $\odot$ in G by the condition

$$a \odot b = a(bb \cdot b) ,$$

the groupoid $< G, \odot >$ is a group.

The purpose of this note is to characterize a group by means of one universal axiom, written in terms of one binary operation (one of the inverse operations of the multiplication).

This problem was solved for the abelian groups by MARLOW SHOLANDER in [5]. He stated that, if the groupoid $< G, - >$ satisfies the condition

$$y = x - [(x - z) - (y - z)] \text{ for all } x, y, z \text{ in } G,$$

then the groupoid $< G, + >$, where $x + y = x - [(y - y) - y]$, is an abelian group.

§ 1. We are going to state the following

THEOREM: *Let* $< \mathrm{G}, \cdot >$ *be a groupoid satisfying the following condition:*

(C) $\mathrm{a} = \mathrm{b}\{[(\mathrm{dd} \cdot \mathrm{a})\mathrm{c}][(\mathrm{dd} \cdot \mathrm{b})\mathrm{c}]\}$ *for all* $\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}$ *in* G.

Then, if one defines the binary operation $\odot$ *in* G *by the condition*

$$\mathrm{a} \odot \mathrm{b} = \mathrm{a}(\mathrm{bb} \cdot \mathrm{b}) \textit{ for all } \mathrm{a}, \mathrm{b} \textit{ in } \mathrm{G},$$

the groupoid $< \mathrm{G}, \odot >$ *is a group.*

PROOF: One has clearly

(1) $a = a\{[(dd \cdot a)c][(dd \cdot a)c]\}$ for all a, c, d in G.

Let us set

$$c = [(dd \cdot b)b][(dd)(dd \cdot a)]b .$$

Since, by condition (C), one has

$$(dd \cdot a)c = (dd \cdot a)(\{[(dd \cdot b)b] \cdot \cdot [(dd)(dd \cdot a)]b\}) = b ,$$

it follows from (1) that

(2) $a = a \cdot bb$ for all a, b in G.

Then, by putting $c = ee$ in (C), one obtains

$$a = b\{[(dd \cdot a)(ee)][(dd \cdot b)(ee)]\}$$

and hence, by (2), one has

$a = b[(dd \cdot a)(dd \cdot b)]$ for all a, b, d in G.

Consequently,

$$aa = (bb)[(dd \cdot aa)(dd \cdot bb)] .$$

From here and (2), it follows

$$aa = (bb)[(dd)(dd)] = (bb)(dd) = bb$$ for all a, b, d in G.

This means that the element bb does not depend on b.

Let us set $i = bb$; then one has

(3) $a = ai$ for every $a \in G$,

that is to say, i is a right identity for the grupoid $< G, \cdot >$.

Thus, the condition (C) may be written

(C′) $a = b[(ia \cdot c)(ib \cdot c)]$ for all a, b, c in G.

By setting $b = c = i$ in (C′), one obtains

$$a = i[(ia \cdot i)(ii \cdot i)]$$

and hence, by (3),

(4) $a = i \cdot ia$ for every $a \in G$.

From (C′) and (4), it results

(5) $ia = (ib)(ac \cdot bc)$ for all a, b, c in G

and, by setting $c = b$, one obtains

(6) $ia = ib \cdot ab$ for all a, b in G.

From (5) it follows, by taking $b = i$,

$$ia = (ii)(ac \cdot ic) = i(ac \cdot ic)$$

and hence, by (4),

(7) $a = ac \cdot ic$ for all a, c in G.

Let us see that one has

(8) $i \cdot ab = ba$ for all a, b in G.

In fact, by (7), (4) and (6), one has

$$ba = b(ab \cdot ib) = (i \cdot ib)(ab \cdot ib) = i \cdot ab .$$