ILLINOIS JOURNAL OF MATHEMATICS
Volume 30, Number 2, Summer 1986

YET ANOTHER SINGLE LAW FOR GROUPS

BY

B.H. NEUMANN

To the memory of my old friend Bill Boone

1. Introduction

Groups can be axiomatised in many ways. Of special interest are definitions of groups in terms of operations and laws, because such a definition has as an immediate consequence the fact that the class of groups forms a variety.

One binary operation suffices, if it is right division,

$$xy\rho = x \cdot y^{-1}$$

(or left division, or the transpose of right division $xy\rho^T = y^{-1} \cdot x$, or the transpose of left division); and in terms of right division (or left division or their transposes), a single, albeit complicated, law suffices: see [1]. If multiplication

$$xy\mu = x \cdot y$$

(or its transpose) is chosen as the binary operation, it does not suffice for a definition of groups by laws; nor even if the nullary operation

$$\varepsilon = e$$

is added. (Greek letters stand for operations and are written as right-hand operators; the nullary ε, operating on the empty sequence on the left-hand side, produces the constant element e, which is to become the neutral element of multiplication, that is the unit element of the group.) If instead the unary inversion

$$x\iota = x^{-1}$$

is added to the binary multiplication, then groups can again be defined by laws, and indeed by a single law: see [2]. In terms of multiplication, inversion, and the nullary unit element, groups can, of course, be defined by laws, but not by a single law: see [2].

Received April 16, 1985.

Recently at the University of Manitoba Dr Padmanabhan asked me whether a single law suffices to define groups in terms of the binary "multiplication of inverses",

$$xy\nu = x^{-1} \cdot y^{-1},$$

and the nullary unit element—that it can be done by laws in these two operations is easy to see. I came away with the impression that Dr Padmanabhan had grounds for thinking that it could not be done; and I soon came to the same conclusion—until I demolished this conclusion by constructing a single law that will do the trick.

As a trick, it is of no real interest, except for a small methodological point in universal algebra: the presence of a nullary operation ensures that all carriers (i.e., sets of elements) of groups are non-empty. We like to forget about the empty set as the carrier of an algebra, but then need to modify the proposition "The intersection of (carriers of) subsemigroups of a semigroup is (the carrier of) a subsemigroup" (usually formulated without my pedanticisms in the parentheses) by the insertion of "if non-empty" before "is" to render it valid. A small price to pay for the convenience of forgetting about the empty set? Perhaps; but the price is not all that small if, for example, we want to turn the power set of the carrier of a semigroup into the carrier of another lattice-ordered semigroup in the obvious way.

This is not a good reason for wanting to axiomatise groups in terms of ν and ε by a single law. However, the gauntlet having been thrown down, somebody had to pick it up.

The notational conventions are as in the earlier papers [1], [2]. Lower case Greek letters stand for algebraic operations; x, y, z, t are variables ranging over the carrier of the algebra under consideration; e, f are constant elements of that carrier; capital letters stand for mappings of the carrier into itself, and I in particular is the identity mapping of the carrier.

Some simple facts that will be used without explicit reference are that if the mapping P of the carrier into itself has both a left inverse and a right inverse, that is if there are mappings Q, Q' with

$$QP = PQ' = I,$$

then $Q = Q'$ is the unique inverse of P, written $Q = P^{-1}$, and P is a permutation of the carrier. Moreover if

$$ABCD = P,$$

where A, D, P are permutations, then B has a right inverse and C has a left inverse. I write mappings as right-hand operators, and read products from left to right; thus a mapping with a right inverse is one-to-one, and a mapping with a left inverse is onto the whole carrier.

2. The law

THEOREM 1. *The law*

$$z\varepsilon y\nu\varepsilon t\nu t\nu x\nu\nu\varepsilon z\nu y\nu\nu\nu = x \tag{1}$$

defines the variety of groups with the interpretation

$$xy\nu = x^{-1} \cdot y^{-1}, \tag{2}$$

$$\varepsilon = e, \text{ the unit element.} \tag{3}$$

The proof follows the pattern of those in [1] and [2]: first I show that with respect to ν the algebra is a quasigroup; next the properties of the element e are investigated; then the associative law for the group multiplication, expressed in terms of ν and ε, is proved; and finally the interpretations (2), (3) of ν and ε are verified. The details follow.

I introduce mappings S_y and T_x of the carrier of the algebra into itself by

$$xy\nu = xS_y = yT_x;$$

they are right and left "ν-multiplication". With this notation the law (1) becomes

$$T_{et\nu t\nu}T_{ey\nu}S_{ez\nu y\nu}T_z = I. \tag{4}$$

This shows that all left ν-multiplications T_z have left inverses, and those of the form $T_{et\nu t\nu}$ also have right inverses, thus are permutations; then also all $T_{ey\nu}$ have right inverses, hence are permutations. Now $ey\nu = yT_e$ ranges with y over the whole carrier, as T_e has a left inverse: this implies that all left ν-multiplications are permutations. Then also all $S_{ez\nu y\nu}$ are permutations; and as $ez\nu y\nu = yT_{ez\nu}$ ranges, even for fixed z, over the whole carrier, all right ν-multiplications S_z are permutations. It follows that with respect to ν the algebra is a quasigroup.

Next it is seen that the mapping $T_{et\nu t\nu}$ $(= T_z^{-1}S_{ez\nu y\nu}^{-1}T_{ey\nu}^{-1})$ does not depend on t, hence is constant; and thus also the element $et\nu t\nu$ is constant. To compute this constant, I introduce the element

$$f = eT_e^{-1},$$

so that $ef\nu = e$. Then the constant element is

$$et\nu t\nu = ef\nu f\nu = ef\nu = e. \tag{5}$$

The law (4) thus implies the simpler law

$$T_eT_{ey\nu}S_{ez\nu y\nu}T_z = I. \tag{6}$$

Next notice that $T_{eyv}S_{ezvyv}$ $(= T_e^{-1}T_z^{-1})$ is independent of y. With $z = f$ this gives that $T_{eyv}S_{eyv}$ is a constant permutation, and putting $eyv = t$ and noting that $t = yT_e^{-1}$ ranges with y over the whole carrier, one has the result that T_tS_t is a constant permutation, say $T_tS_t = K$. With $z = f$ then (6) gives

$$T_eKT_f = I.$$

Put $t = e$ in (5) to get

$$eevev = eT_eS_e = eK = e; \tag{7}$$

and, still using (5),

$$etvtv = e = eK = eT_tS_t = tevtv.$$

Hence $etv = tev$, or $tT_e = tS_e$: thus

$$T_e = S_e. \tag{8}$$

Now from (7), $e = eK^{-1} = eT_fT_e$, that is

$$eevev = e = efevv = fevev.$$

Hence $fev = eev$ and $f = e$; and, moreover, $eev = e$. Now (8) shows that $K = T_eS_e = T_e^2$, and $T_e^4 = I$. This is not quite good enough: what is needed is $K = T_e^2 = I$. To show this, put $y = z$ in (6), notice that $ezvzv = e$ and use (8) again:

$$T_eT_{eyv}T_eT_y = I. \tag{9}$$

Multiply on the right by S_yT_e and use $T_eT_yS_yT_e = T_eKT_e = I$, to get

$$T_eT_{eyv} = S_yT_e. \tag{10}$$

Replace y in (9) by eyv; then

$$T_{eeyvv} = T_e^{-1}T_{eyv}^{-1}T_e^{-1} = T_y.$$

Hence $eeyvv = y$, that is $yT_e^2 = y$, and

$$T_e^2 = I, \tag{11}$$

as required. This implies $K = I$, and

$$S_t = T_t^{-1} \tag{12}$$

for all t.

Now define a new operation μ by

$$xy\mu = yx\nu\varepsilon\nu.$$

With the notation

$$xy\mu = xR_y = yL_x,$$

it is seen that

$$R_y = T_yS_e, \quad L_x = S_xS_e,$$

so R_y, L_x are permutations, and the algebra is a quasigroup with respect to μ. Next,

$$xyz\mu\mu = zy\nu\varepsilon\nu x\nu\varepsilon\nu = xT_{zy\nu e\nu}S_e \tag{13}$$

and

$$xy\mu z\mu = zyx\nu\varepsilon\nu\nu\varepsilon\nu = xT_yS_eT_zS_e; \tag{14}$$

now

$$zy\nu\varepsilon\nu = zS_yS_e = zS_yT_e = zT_eT_{ey\nu} = ey\nu ez\nu\nu$$

by (10), and

$$\begin{aligned} T_{ey\nu ez\nu\nu} &= S^{-1}_{ey\nu ez\nu\nu} = T_yT_eT_{eez\nu\nu} \\ &= T_yT_eT_z = T_yS_eT_z, \end{aligned}$$

using (12), (6), (11), (8). It follows that the right-hand sides of (13) and (14) are equal, verifying the associative law for μ. Next,

$$xe\mu = ex\nu e\nu = xT_eS_e = xT_e^2 = x$$

and

$$ex\mu = xe\nu e\nu = xS_e^2 = xT_e^2 = x,$$

showing that e is the (right and left) neutral element with respect to μ. Also

$$xex\nu\mu = ex\nu x\nu e\nu = ee\nu = e,$$

by (5), so $ex\nu$ is the (right, hence also left) inverse of x with respect to μ and e. This shows the group property of the algebra with respect to μ as multiplication, with e as unit element and $ex\nu$ as inverse of x. Finally, to verify the interpretations (2) and (3) of ν and ε: that of ε has just been verified, and it remains to show that

$$ey\nu ex\nu\nu e\nu = xy\nu.$$

Here the left-hand side is $xT_eT_{eyv}S_e = xS_y$, by (10) and (12), giving the desired interpretation, and so completing the proof of the theorem.

3. Final remarks

The law (1) has a word of length 19 as its left-hand side—counting, as one has to in the presence of nullary or unary operations, both Latin and Greek letters. Is 19 the least possible length? I do not know the answer. The number of variables involved in (1) is 4; can this be reduced to 3? I do not know the answer. Can one, as in the single group laws of [1] and [2], build a further law into (1), so as to define a subvariety of the variety of all groups, for example the variety of all abelian groups, by a single law in ν and ε? I have not tried, but guess that this should be quite feasible. Can one define the variety of groups by a single law in ν and ι, where ι is inversion, $x\iota = x^{-1}$? This question can be answered in the affirmative:

THEOREM 2. *The law*

$$tzy\nu zx\iota y\iota\nu\nu\iota\nu\nu t\nu\iota = x$$

defines the variety of groups with the interpretation

$$xy\nu = x^{-1} \cdot y^{-1}, \quad x\iota = x^{-1}.$$

The proof follows lines similar to that of Theorem 1, and is omitted. The same questions can be asked about the law in Theorem 2 as about the law in Theorem 1; I know no more answers. Finally one may wish to define groups by a single law in right division, $xy\rho = x \cdot y^{-1}$, and either ε or ι; this should be quite feasible, but I have not tried.

REFERENCES

1. GRAHAM HIGMAN and B.H. NEUMANN, *Groups as groupoids with one law*. Publ. Math. Debrecen, vol. 2 (1952), pp. 215–221.
2. B.H. NEUMANN, *Another single law for groups*, Bull. Austral. Math. Soc., vol. 23 (1981), pp. 81–102.

AUSTRALIAN NATIONAL UNIVERSITY
CANBERRA, AUSTRALIA

COMMONWEALTH SCIENTIFIC AND INDUSTRIAL RESEARCH ORGANIZATION
CANBERRA, AUSTRALIA