BULL. AUSTRAL. MATH. SOC.
VOL. 23 (1981), 81-102.

20A05
(08B05, 20E10)

ANOTHER SINGLE LAW FOR GROUPS

B.H. NEUMANN

It has long been known that, in terms of right division, groups can be defined by a single law. In this paper a single law defining groups in terms of multiplication and inversion is proposed. This law is in 4 variables, and it is conjectured that no fewer than 4 variables will do, and that the proposed law is of minimal length as well. Some extensions of the result, and an alternative single law with the same length and number of variables, are also discussed. By contrast, groups in terms of multiplication, inversion, and a unit element can not be defined by a single law. Most of these results were stated by Tarski at the Logic Colloquium at Hannover in 1966, but apparently no proof has yet been published.

1. Introduction

In [3, p. 280], Alfred Tarski states that groups can be defined by a single law in terms of multiplication and inversion, but not in terms of multiplication, inversion, and a unit element. However, I am not aware of any published proof of these results, and in this paper I provide such a

Received 7 August 1980. The author is greatly indebted, and deeply grateful, to Professor Narain D. Gupta and to the Department of Mathematics and Astronomy at the University of Manitoba, Winnipeg, for hospitality during the autumn semester 1979, when some of this work was carried out. Some was also done while the author enjoyed the hospitality, in March 1980, of the Department of Mathematics of Nanyang University, Singapore (now part of the National University of Singapore). The author also thanks Professor R. Padmanabhan for many stimulating discussions, and for drawing his attention to Tarski's paper and priority. Finally the author acknowledges the collaboration of Dr L.J. Hesterman in a much earlier, unsuccessful attack on the problem here treated.

proof. Tarski's approach is through logic, while mine is only algebraic; our notations are rather different; and we even differ in terminology, as Tarski calls "left-hand division" what I call "right division". I shall therefore develop the subject in my own pedestrian manner.

It was first shown in [2] that groups can be defined by a single law in a binary operation, namely right division. This raises the problem of defining groups by a single law in a binary operation, namely multiplication, and a unary operation, namely inversion; or in terms of a binary multiplication, a unary inversion, and a nullary operation giving the unit element. I denote operations by lower case Greek letters, and use, in particular, ρ for right division, μ for multiplication, ι for inversion, and ε for the nullary operation that gives the unit element (though a different notation will be used, most of the time, for the unit element, because elements and element variables will be denoted by lower case italic litters). I use what is now called the "inverse Polish" notation; thus

$$ab\rho \ , \quad ab\mu \ , \quad a\iota \ , \quad \varepsilon$$

stand for the results of operating on the (ordered) pair (a, b) with ρ, or with μ, or on a with ι, or on the empty sequence with ε, respectively. However, ε will be used in Appendix B only.

Now in a group with multiplication μ and inversion ι, right division is given by

$$xy\rho = xy\iota\mu \ ; \tag{1.1}$$

and μ and ι can be expressed in terms of ρ by

$$x\iota = xx\rho x\rho \ , \tag{1.2}$$

$$xy\mu = xyy\rho y\rho\rho \ . \tag{1.3}$$

Thus the law

$$xxx\rho y\rho z\rho xx\rho x\rho z\rho\rho\rho = y \ ,$$

proved in [2] to define the variety of groups, can be immediately translated into a law in μ and ι, by simply replacing ρ by $\iota\mu$ at each of its occurrences, namely

$$xxx\iota\mu y\iota\mu z\iota\mu xx\iota\mu x\iota\mu z\iota\mu\iota\mu\iota\mu = y \ . \tag{1.4}$$

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

But though the variety so defined is the variety of groups in some sense, it is not the variety of groups in terms of μ as multiplication and ι as inversion: it is the variety of groups in terms of a new multiplication μ^*, say, and a new inversion ι^*, say, defined, in analogy to (1.2) and (1.3) by

$$x\iota^* = xx\iota\mu x\iota\mu ,$$

$$xy\mu^* = xyy\iota\mu y\iota\mu\iota\mu .$$

There is no reason why (1.4) should imply $\iota^* = \iota$ or $\mu^* = \mu$; and indeed the following model shows that such an implication is not true:

Let G be a group with multiplication μ^* and inversion ι^*, and assume the centre of G contains an element c of order 2. Define

$$x\iota = x\iota^* c\mu^* ,$$

$$xy\mu = xy\mu^* .$$

Then the law (1.4) will be satisfied in G, because though at each occurrence of ι an extra factor c is inserted in the left-hand side, all these factors can be combined to a single power of c, because c is central. Note that some of the factors c may be inverted by some of the operations ι that occur: but as c is of order 2, this does not change them. The final power of c that collects is even, because there are 8 occurrences of ι in (1.4); but as c is of order 2, this even power equals the neutral element, and thus can be omitted. Thus (1.4) is satisfied; but ι manifestly is not inversion with respect to μ as multiplication.

This same model shows more generally:

LEMMA 1. *If a set of laws in μ and ι defines the variety of groups, then the number of occurrences of ι in at least one of the laws must be odd.* //

Various modifications of the law (1.4) have been tried, without success. I propose, therefore, a quite different law, which involves 4 variables as against only 3 in the law (1.4):

THEOREM 1. *The variety of groups is defined, in terms of multiplication μ and inversion ι, by the single law*

(1.5) $$xy\iota x\iota t\mu\mu\iota z\mu yz\mu\iota\mu\iota\mu = t .$$

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

Here, as always, x, y, z, t are variables that range over the set of elements, or *carrier*, of the (μ, ι) algebra considered, and a law like (1.5) is interpreted as the sentence that results from binding all variables by universal quantifiers.

The law (1.5) is not the only one that will serve to define the variety of groups; another can readily be derived from it by the observation that a (μ, ι) group is also a (μ^{-1}, ι) group, where μ^{-1} is defined by

$$xy\mu^{-1} = yx\mu \ ;$$

and there are other ways of shuffling variables and operations.

There is, however, a different single law in μ and ι that can not be so derived from (1.5):

THEOREM 2. *The variety of groups is defined, in terms of multiplication* μ *and inversion* ι *, by the single law*

$$zz\iota\mu\iota x t\mu y\mu\iota x\mu\iota y\iota\mu\mu = t \ . \tag{1.6}$$

The proofs of Theorems 1 and 2 are similar in some respects, different in others. One point of similarity is that neither of them is interesting. Nevertheless I shall give the proof of Theorem 1 later in this paper; the proof of Theorem 2 is relegated to Appendix A.

2. Other varieties of groups

A subvariety of the variety of all groups that can be defined by a finite system of group laws can also be defined by a single group law. Such varieties, which I call *mononomic* varieties of groups, were treated in [2] simultaneously with the variety of all groups; they were of greater interest when [2] was written than they are now, because then no other group varieties were known yet.

Theorem 1 can be extended to mononomic varieties of groups. So can Theorem 2, though some slight extra complication seems then to become necessary.

Let

$$u = v \tag{2.1}$$

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

be a group law, where u and v are (μ, ι) words in variables $x_1, x_2, \ldots, x_n$. Put $uv\iota\mu = w$, so that w is also a (μ, ι) word in $x_1, x_2, \ldots, x_n$, and the law (2.1) is equivalent to

$$w = e \ , \tag{2.2}$$

where e is the unit element (whose existence is yet to be established). Denote by w' the word obtained from w by replacing $x_1, x_2, \ldots, x_n$ by $x_1', x_2', \ldots, x_n'$, respectively. Then the analogue of Theorem 1 is:

THEOREM 3. *The mononomic variety of groups with the law* (2.1) *is defined, in terms of multiplication* μ *and inversion* ι, *by the single law*

$$xy\iota x\iota t\mu\mu\iota z\mu yz\mu\iota\mu ww'\iota\mu\iota\mu\iota\mu = t \ . \tag{2.3}$$

The law (2.3) differs from (1.5) by the insertion of a factor $ww'\iota\mu\iota$, which will later be shown to be constant with value e (before e has been shown to be the unit element of μ). The form of the factor is designed to ensure that the total number of occurrences of ι on the left-hand side of the law remains odd, as by Lemma 1 it has to be.

To modify Theorem 2 analogously, a further additional variable z' is required:

THEOREM 4. *The mononomic variety of groups with the law* (2.1) *is defined, in terms of multiplication* μ *and inversion* ι, *by the single law*

$$zz\iota\mu\iota z'z'\iota\mu\iota ww'\iota\mu\iota xt\mu y\mu\iota x\mu\iota y\iota\mu\mu\mu = t \ . \tag{2.4}$$

The proof of this theorem is, like that of Theorem 2, relegated to Appendix A.

The variety of abelian groups, in particular, can be defined by a single law of the form (2.3) or (2.4), with $w = x_1x_2\mu x_2x_1\mu\iota\mu$. In [2], a shorter and simpler law in terms of right division ρ was shown to suffice. I have not been able to find a corresponding shorter or simpler law to define the variety of abelian groups in terms of μ and ι, though a minor simplification is possible by replacing the factor $ww'\iota\mu\iota$ in (2.3) or (2.4) by a factor w^* defined by

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

(2.5) $$w^* = x_1 x_2 \mu x_2 x_1 \mu\iota\mu\iota \ .$$

The question naturally arises whether the variety of groups can be defined by a single law in terms of a binary multiplication μ, a unary inversion ι, and a nullary unit element ε. This is, in fact not the case, as already stated by Tarski [3]; a proof is presented in Appendix B.

3. The quasigroup property

Mappings of the carrier of a (μ, ι) algebra into itself are denoted by capital letters, and in particular the identity mapping is I. If a mapping P has both a left inverse and a right inverse, then P is a permutation of the carrier, and its (unique left and right) inverse is denoted by P^{-1}. The following well-known fact is used repeatedly.

LEMMA 2. *If*

$$ABCD = E \ ,$$

where A, D, and E are permutations, then B has a right inverse and C has a left inverse. //

The binary operation μ gives rise to the *right multiplications* R_a, defined for every element a of the carrier by

$$xR_a = xa\mu \ ,$$

and the *left multiplications* L_a, defined correspondingly by

$$xL_a = ax\mu \ .$$

The unary operation ι defines a mapping O, the *opposition* (mapping x to its *opposite*),

$$xO = x\iota \ .$$

In terms of these mappings, the law (1.5) can be reformulated as

(3.1) $$L_{x\iota} L_{y\iota} O R_z R_{yz\mu\iota} O L_x = I \ .$$

Similarly the law (2.3) becomes

(3.2) $$L_{x\iota} L_{y\iota} O R_z R_{yz\mu\iota} R_{ww'\iota\mu\iota} O L_x = I \ .$$

These two laws can be combined in the form

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

(3.3) $$L_{x\iota}L_{y\iota}OR_zR_{yz\mu\iota}XOL_x = I \ ,$$

where $X = I$ in (3.1) and $X = R_{ww'\iota\mu\iota}$ in (3.2), so that almost all of the proofs of Theorems 1 and 3 can proceed simultaneously, starting from (3.3).

The first step is to prove the following fact:

LEMMA 3. *A* (μ, ι) *algebra subject to the law* (3.3) *is a quasigroup with respect to* μ, *and* O *is a permutation of its carrier.*

Note. For terms such as *quasigroup*, *loop*, or *inverse property*, the survey [1] by Bruck may be consulted.

Proof of Lemma 3. Repeated use of Lemma 2 applied to (3.3) shows that L_x has a left inverse, for every x, and $L_{x\iota}$ has a right inverse: thus $L_{x\iota}$ is a permutation, and so then, of course, is $L_{y\iota}$. Then O has a right inverse. Choose $x = x'\iota$, so that L_x is also a permutation; then O has a left inverse for this choice of x, on which, however, it does not depend: so *opposition is a permutation*. In particular then x ranges over the whole carrier, and thus *all left multiplications are permutations*. This means that, for every a, b in the carrier, the equation

$$xL_a = b \ ,$$

or

$$ax\mu = b \ ,$$

has a unique solution x.

Again Lemma 2 is used repeatedly: first R_z has a right inverse for every z, and X has a left inverse. If $X = R_{ww'\iota\mu\iota}$, then X is thus a permutation; if $X = I$, then X is trivially also a permutation. Thus $R_{yz\mu\iota}$ has a left inverse. But $yz\mu\iota = zL_yO$ ranges over the whole carrier: thus *all right multiplications are permutations*. This means that, for every a, b in the carrier, the equation

$$xR_a = b \ ,$$

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

or

$$xa\mu = b \ ,$$

has a unique solution x . The algebra is then a quasigroup with respect to μ , and Lemma 3 follows. //

From now on, the inverses of left and right multiplications and of opposition can be freely used. In particular, for any elements a, b, c of the carrier, the implications

(3.4) *if* $ab\mu = ac\mu$, *then* $b = c$,

(3.5) *if* $ba\mu = ca\mu$, *then* $b = c$, and

(3.6) *if* $b\iota = c\iota$, *then* $b = c$

will be used frequently.

4. An idempotent element

Note that $R_z R_{yz\mu\iota}$ does not depend on z , because

$$R_z R_{yz\mu\iota} = O^{-1}L_{y\iota}^{-1}L_{x\iota}^{-1}L_x^{-1}O^{-1}\chi^{-1} \ ,$$

and z does not occur on the right-hand side. Hence

(4.01) $$tz\mu yz\mu\iota\mu = ts\mu ys\mu\iota\mu \ .$$

Here put $y = t$ and choose z and s so that, for arbitrarily given u and v ,

$$tz\mu = u \ , \quad ts\mu = v \ ;$$

that is to say, put $z = uL_t^{-1}$, $s = vL_t^{-1}$. Then (4.01) becomes

$$uu\iota\mu = vv\iota\mu \ .$$

This is thus a constant element, say

(4.02) $$uu\iota\mu = f \ .$$

Putting $f\iota = e$ and $fO^{-1} = g$, then

(4.03) $$gf\mu = fe\mu = f \ .$$

These elements will later be shown to be all equal.

Next observe that, as the variables in w and in w' are distinct

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

from the variables without suffixes, X is a constant element,

$$X = R_{yz\mu\iota}^{-1} R_z^{-1} O^{-1} L_{y\iota}^{-1} L_{x\iota}^{-1} L_x^{-1} O^{-1} .$$

In the case of Theorem 1, this is the identity permutation, $X = I$. In the case of Theorem 3 it is

$$X = R_{ww'\iota\mu\iota} ,$$

which will eventually turn out to be the identity permutation, too. However, it follows already now that $ww'\iota\mu\iota$ is a constant element. To evaluate it, put $x_1' = x_1$, $x_2' = x_2$, ..., $x_n' = x_n$, so that $w' = w$. Then $ww\iota\mu = f$, $ww\iota\mu\iota = e$, and thus also $ww'\iota\mu\iota = e$, and

$$X = R_e . \tag{4.04}$$

It is clear, incidentally, that w must be itself be a constant element, whose evaluation will, however, have to wait.

Transform (3.3) by L_x, and note that

$$L_x L_{x\iota} = O^{-1} X^{-1} R_{yz\mu\iota}^{-1} R_z^{-1} O^{-1} L_{y\iota}^{-1}$$

does not depend on x, and thus is a constant permutation. To evaluate it, consider

$$zL_x L_{x\iota} = zL_y L_{y\iota} ,$$

that is

$$x\iota xz\mu\mu = y\iota yz\mu\mu ,$$

and choose $y = zO^{-1}$, so that $y\iota = z$. Then

$$x\iota xz\mu\mu = zyy\iota\mu\mu = zf\mu ,$$

that is to say

$$L_x L_{x\iota} = R_f . \tag{4.05}$$

With this, (3.3) transformed by L_x becomes

$$R_f L_{y\iota} OR_z R_{yz\mu\iota} XO = I . \tag{4.06}$$

Put $z = y\iota$ here, so that $yz\mu\iota = e$; then (4.06) becomes

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

(4.07) $$R_f L_{y1} O R_{y1} R_e X O = I .$$

Now

$$L_{y1} O R_{y1} = R_f^{-1} O^{-1} X^{-1} R_e^{-1}$$

is independent of y, that is to say, a constant permutation. To evaluate it, consider

$$z L_{y1} O R_{y1} = z L_{x1} O R_{x1} ,$$

that is

$$y_1 z \mu_1 y_1 \mu = x_1 z \mu_1 x_1 \mu ,$$

and choose x so that $x_{11} = z$, or $x_1 = z O^{-1}$. Then

$$y_1 z \mu_1 y_1 \mu = x_1 x_{11} \mu_1 z O^{-1} \mu = e z O^{-1} \mu ,$$

that is

$$L_{y1} O R_{y1} = O^{-1} L_e .$$

Substitute this in (4.07) to get

$$R_f O^{-1} L_e R_e X O = I ,$$

or

(4.08) $$L_e R_e X O R_f = O .$$

Here the value of X needs to be used. As $X = I$ in the case of (3.1) (or Theorem 1) and $X = R_e$ in the case of (3.2) (or Theorem 3) - see (4.04) - , put $X = R_e^p$, where $p = 0$ or $p = 1$. Then (4.09) becomes

$$L_e R_e^{p+1} O R_f = O ,$$

or

$$e z \mu e \mu \ldots e \mu_1 f \mu = z_1 ,$$

where $e\mu \ldots e\mu$ stands for $p + 1$ factors $e\mu$. In this, put $z = e_1$, so that $ez\mu = ee_1\mu = f$, then

$$f e \mu \ldots e \mu_1 f \mu = e_{11} .$$

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

Note that $fe\mu \ldots e\mu = f$, however many factors $e\mu$ there are. Thus

$$f\iota f\mu = e\iota\iota ,$$

or, finally,

$$ef\mu = e\iota\iota . \tag{4.09}$$

Next use (4.02), (4.03), (4.05), (3.4):

$$x\iota x\iota\iota\mu = f = gf\mu = gR_f = gL_xL_{x\iota} = x\iota xg\mu\mu ,$$

so that

$$x\iota\iota = xg\mu , \tag{4.10}$$

that is

$$O^2 = R_g . \tag{4.11}$$

Apply (4.10) to (4.09), and then (3.4):

$$ef\mu = e\iota\iota = eg\mu ,$$

whence $f = g$; and applying opposition to both sides, also $e = f$. This proves

$$e = f = g , \tag{4.12}$$

and thus also

$$ee\mu = e\iota = e . \tag{4.13}$$

To sum up:

LEMMA 4. *A* (μ, ι) *algebra subject to the law* (3.3) *contains an idempotent element* e *with respect to* μ *which is invariant under* ι *and satisfies, for all* x *,*

$$xx\iota\mu = e . \tag{4.14}$$ //

5. The inverse loop property

Return briefly to the situation of Theorem 3. It has already been remarked that $w = w(x_1, x_2, \ldots, x_n)$ is a constant element, and, of course, equal to w' . To evaluate this constant, put $x_1 = x_2 = \ldots = x_n = e$. Repeated application of Lemma 4 then shows that

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

(5.1) $$w = e ,$$

which is (2.2) - except that it still remains to be proved that e is the μ unit element. To prove this, start from (4.07), with f replaced by e and X replaced by R_e^p :

(5.2) $$R_e L_{y_1} O R_{y_1} R_e^{p+1} O = I ,$$

and apply this to e :

$$y_1 e e \mu \mu_1 y_1 1 \mu e \mu \ldots e \mu 1 = e ,$$

where again $e\mu \ldots e\mu$ stands for $p + 1$ factors $e\mu$. This immediately simplifies, by (4.13) and the permutation properties of R_e and O , to

$$y_1 e \mu 1 y_1 1 \mu = e = y y_1 1 \mu$$

by (4.14). Apply (3.5) to obtain

$$y_1 e \mu 1 = y ,$$

or

$$O R_e O = I .$$

This combines with (4.11), with g replaced by e , to

$$O^4 = R_e^2 = I ,$$

and it also implies that R_e and O commute. Use this commutativity in (5.2) with $y_1 = e$, transformed by R_e , together with (4.11), to get

$$L_e R_e^{p+3} = I .$$

This gives

(5.3) $$L_e = R_e$$

if p is even,

(5.4) $$L_e = I$$

if p is odd. Now (4.05), with $x = x1 = f = e$, that is

(5.5) $$L_e^2 = R_e ,$$

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

combines with (5.3) to give

$$L_e = I \tag{5.4}$$

also in the case that p is even; and (5.4) and (5.5) combine to give also

$$R_e = I \ . \tag{5.6}$$

Thus e is the (unique) unit element of μ, and from (4.11) then

$$O^2 = I \ . \tag{5.7}$$

This shows:

LEMMA 5. *A* (μ, ι) *algebra subject to the law* (3.3) *is an inverse property loop with unit element* e *and inversion* ι . //

6. Associativity

Now (4.05) becomes

$$L_x L_{x\iota} = I \ ; \tag{6.1}$$

and (4.06), with $y = e$ and all identity permutations on the left-hand side omitted, becomes

$$OR_z R_{z\iota} O = I \ ,$$

which after transformation by O and application of (5.7) gives

$$R_z R_{z\iota} = I \ . \tag{6.2}$$

Now (5.2), with all factors $R_e = I$ omitted, is

$$L_{y\iota} OR_{y\iota} O = I \ ,$$

or, with the involutory property (5.7) of opposition

$$L_{y\iota} OR_{y\iota} = O \ .$$

Apply this to $x\iota$ to get

$$y\iota x\iota\mu\iota y\iota\mu = x\iota\iota = x \ .$$

Then

$$y\iota x\iota\mu\iota y\iota\mu y\mu = xy\mu \ .$$

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

The left-hand side is

$$y\imath x\imath\mu\imath R_{y\imath}R_{y} = y\imath x\imath\mu\imath \ ,$$

by (6.2) with $z = y\imath$. Thus

$$y\imath x\imath\mu\imath = xy\mu \ . \tag{6.3}$$

Now return to (4.06), with the factors $R_f = X = I$ omitted:

$$L_{y\imath}{}^{O}R_{z}R_{yz\mu\imath}{}^{O} = I \ ,$$

and apply this to $x\imath$:

$$y\imath x\imath\mu\imath z\mu yz\mu\imath\mu\imath = x\imath \ ,$$

or, using (3.6) and (6.3),

$$xy\mu z\mu yz\mu\imath\mu = x \ .$$

Then

$$xy\mu z\mu yz\mu\imath\mu yz\mu\mu = xyz\mu\mu \ .$$

Here the left-hand side is, by (6.2) with $yz\mu\imath$ in place of z ,

$$xy\mu z\mu R_{yz\mu\imath}R_{yz\mu} = xy\mu z\mu \ ;$$

so finally the associative law

$$xy\mu z\mu = xyz\mu\mu \tag{6.4}$$

for μ is proved. This shows that the $(\mu, \imath)$ algebra is a group with μ as multiplication and $\imath$ as inversion.

To complete the proof of Theorem 1, it is necessary to verify that the law (1.5) is satisfied in groups; this verification is straightforward and omitted. //

In the case of Theorem 3, it has already been shown that the law (2.2) follows from the law (2.3) - see (5.1). Thus again it only remains to verify that the law (2.3) is satisfied in groups with the law (2.1) or equivalently (2.2); again this verification is straightforward and omitted. //

Appendix A. Proof of Theorems 2 and 4

The laws (1.6) in Theorem 2 and (2.4) in Theorem 4 can be

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

reformulated, in analogy with (3.3), in the form

$$L_x R_y O R_x O R_{y\iota} X L_{zz\iota\mu\iota} = I \ , \tag{A.01}$$

where $X = I$ in the case of Theorem 2 and $X = L_{ww'\iota\mu\iota} L_{z'z'\iota\mu\iota}$ in the case of Theorem 4.

As before, the μ quasigroup property and the fact that opposition is a permutation are established first, by repeated application of Lemma 2. First all L_x have right inverses, and all $L_{zz\iota\mu\iota}$ have left inverses, too, and thus are permutations. Then X, being either the identity and thus trivially a permutation, or a product of two permutations of the form $L_{zz\iota\mu\iota}$, is also a permutation. Put $x = x'x'\iota\mu\iota$, so that L_x becomes a permutation. Then R_y has a right inverse and $R_{y\iota}$ a left inverse - but y and $y\iota$ do not depend on the particular choice of x; thus all R_y have right inverses, and all $R_{y\iota}$ are permutations. Put $y = y'\iota$ to ensure that R_y is also a permutation; then O, which does not depend on the special choices of x and y, is seen to have both right and left inverses and thus is also a permutation. In particular $y = y'\iota$ ranges with y' over the whole carrier; hence all right multiplications are permutations. Return to (A.01) with arbitrary x; now all mappings that occur, except the left-most factor L_x, have been shown to be permutations. It follows that L_x is also a permutation, that is all left multiplications are permutations, and the analogue of Lemma 3, with the law (A.01) in place of (3.3), is established.

Next observe that

$$L_{zz\iota\mu\iota} = X^{-1} R_{y\iota}^{-1} O^{-1} R_x^{-1} O^{-1} R_y^{-1} L_x^{-1}$$

is seen to be independent of z, hence a constant permutation; and again it follows that

$$zz\iota\mu\iota = e \ ,$$

say, is a constant element. As before, put $f = eO^{-1}$, $g = fO^{-1}$, so that again

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

$$zz\iota\mu = f = gf\mu = fe\mu \ .$$

In the situation of Theorem 4, put $x_1' = x_1$, $x_2' = x_2$, ..., $x_n' = x_n$, so that $w' = w$. Then $ww'\iota\mu\iota = e$; and as also $z'z'\iota\mu\iota = e$, then

$$X = L_e^2$$

in this situation. In the case of the variety of all groups, that is in Theorem 2, $X = I$, so

$$X = L_e^p$$

with $p = 0$ or $p = 2$ will cover both cases. Note that p is even: this fact will be used later. (A.01) now simplifies to

$$L_x R_y O R_x O R_{y\iota} L_e^{p+1} = I \ . \tag{A.02}$$

Here

$$L_x R_y O R_x = L_e^{-(p+1)} R_{y\iota}^{-1} O^{-1}$$

is seen to be independent of x; thus

$$xz\mu y\mu\iota x\mu = tz\mu y\mu\iota t\mu \ .$$

Put $t = zO^{-1}$, so that $z = t\iota$. Then

$$xt\iota\mu y\mu\iota x\mu = fy\mu\iota t\mu \ .$$

Here put $x = y = e$, and observe that then $fy\mu\iota = fe\mu\iota = e$. Then

$$et\iota\mu e\mu\iota e\mu = et\mu \ ,$$

or

$$OL_e R_e O R_e = L_e \ . \tag{A.03}$$

Returning to (A.02), notice that

$$R_y O R_x O R_{y\iota} = L_x^{-1} L_e^{-(p+1)}$$

is independent of y; thus

$$zy\mu\iota x\mu\iota y\iota\mu = zt\mu\iota x\mu\iota t\iota\mu \ .$$

Put $t = z\iota$, so that $zt\mu\iota = zz\iota\mu\iota = e$; thus

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

(A.04) $$zy\mu\iota x\mu\iota y\iota\mu = ex\mu\iota z\iota\iota\mu \ .$$

Here put $z = ex\mu$, so that the right-hand side reduces to f :

$$ex\mu y\mu\iota x\mu\iota y\iota\mu = f = yy\iota\mu \ .$$

Cancelling on the right, that is to say, applying (3.5), which is available because the analogue of Lemma 3 has already been established, then

(A.05) $$ex\mu y\mu\iota x\mu\iota = y \ ,$$

and with $y = e$ in particular

$$ex\mu e\mu\iota x\mu\iota = e = f\iota \ ,$$

and by (3.6),

$$ex\mu e\mu\iota x\mu = f = xO^{-1}x\mu \ .$$

Again by (3.5) then

$$ex\mu e\mu\iota = xO^{-1} \ ,$$

or

$$ex\mu e\mu\iota\iota = x \ .$$

This means that

(A.06) $$L_e R_e O^2 = I \ .$$

Transform by O to obtain

(A.07) $$OL_e R_e O = I \ .$$

This combines with (A.03) to give

(A.08) $$R_e = L_e \ .$$

Note that as $fe\mu = f$, that is to say $fR_e = f$, also now for all n ,

(A.09) $$fR_e^n = fL_e^n = f \ .$$

In particular

(A.10) $$ef\mu = f = gf\mu \ ,$$

whence, by (3.4),

$$e = g = e\iota\iota \ ,$$

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

and so also

(A.11) $$f\iota\iota = e\iota = g\iota = f \ .$$

Return to (A.02), applied to a variable z :

$$xz\mu y\mu\iota x\mu\iota y\iota\mu L_e^{p+1} = z \ ,$$

and put $y = xz\mu\iota$, so that $xz\mu y\mu\iota = e$. Then

$$ex\mu\iota xz\mu\iota\iota\mu L_e^{p+1} = z \ .$$

Here put $x = f$ and $z = e$ and use (A.10) and (A.11) to get

$$ef\mu\iota fe\mu\iota\iota\mu L_e^{p+1} = ef\iota\iota\mu L_e^{p+1} = e \ ,$$

that is

$$fL_e^{p+1} = e \ ,$$

and by (A.09) finally

$$f = e \ .$$

This establishes, as before,

$$e = f = g$$

and

$$ee\mu = e\iota = e \ ,$$

and the analogue of Lemma 4, with the law (A.01) in place of (3.3).

In (A.05), put $x = e$, and obtain

$$ey\mu\iota e\mu\iota = y \ ,$$

or

$$L_e O R_e O = I \ .$$

Compare this with (A.07) to see that L_e , which by (A.08) equals R_e , commutes with O :

(A.12) $$L_e O = O L_e \ .$$

In (A.04), put $x = y = e$, to get

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

$$ze\mu_1 e\mu_1 e\mu = ez_1 1\mu \ ,$$

or

$$R_e O R_e O R_e = L_e O^2 \ .$$

Using (A.08) and the commutativity (A.12), this gives

(A.13) $$L_e^2 = I \ ,$$

and with (A.06) and again (A.08) also

(A.14) $$O^2 = I \ .$$

Now put $x = y = e$ in (A.02) to get

$$L_e R_e O R_e O R_e L_e^{p+1} = I \ .$$

Use (A.08), (A.12), (A.13), and (A.14) to deduce

$$L_e^{p+1} = I$$

from this; and now recall that p is even, namely $p = 0$ or $p = 2$, and apply (A.13) to obtain finally

(A.15) $$L_e = I \ .$$

Now the analogue of Lemma 5, with the law (3.3) replaced by (A.01), follows; and (A.02) further reduces to

(A.16) $$L_x R_y O R_x O R_{y_1} = I \ .$$

Put $x = e$ and use (A.15) and (A.14):

(A.17) $$R_y R_{y_1} = I \ .$$

Thus also $R_{y_1} R_y = I$, and multiplying the two sides of (A.16) by R_y gives

$$L_x R_y O R_x O = R_y \ .$$

Then

(A.18) $$xz\mu y\mu_1 x\mu_1 = zy\mu \ .$$

Put $z = x_1$, so that, by (A.14), $x = z_1$, and observe that the factor

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

$xz\mu = e$ can be omitted:

(A.19) $$y\imath z\imath\mu\imath = zy\mu \ ,$$

which, but for the name of one of the variables, is (6.3). Now apply $\imath$ to both sides of (A.18), observing (A.14):

$$xz\mu y\mu\imath x\mu = zy\mu\imath \ .$$

Next

$$xz\mu y\mu\imath x\mu x\imath\mu = zy\mu\imath x\imath\mu \ .$$

Here the left-hand side simplifies, using (A.17),

$$xz\mu y\mu\imath R_x R_{x\imath} = xz\mu y\mu\imath \ ,$$

whence

$$xz\mu y\mu\imath = zy\mu\imath x\imath\mu \ .$$

Apply opposition to both sides, observing (A.14):

$$xz\mu y\mu = zy\mu\imath x\imath\mu\imath \ ,$$

and apply (A.19) to this, with $zy\mu$ in place of y and x in place of z, to get finally

$$xz\mu y\mu = xzy\mu\mu \ .$$

This is the associative law for μ, completing the proof of the group property. To complete the proof of Theorems 2 and 4, it is again necessary to verify that the law (1.6) holds in groups, and that the law (2.4) holds in groups with the law (2.1) or equivalently (2.2). Again this verification is routine, and omitted. //

Appendix B. A nullary unit element

One might hope to be able to go one step further and define groups also by a single law in a binary multiplication μ, a unary inversion $\imath$, and a nullary unit element ε; this is, however, not possible, as stated by Tarski [3], and as I shall now show.

THEOREM 5. *Let*

(B.1) $$w(x, y_1, y_2, \ldots, y_n) = x$$

be a law in variables $x, y_1, y_2, \ldots, y_n$ *with operations* μ *(binary),* $\imath$

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

(unary), ε (nullary) that is satisfied in groups when μ is interpreted as multiplication, ι as inversion, and ε as the unit element. Then this law is also satisfied in a group with μ as multiplication, but ε not as unit element; in this model ι may or may not be inversion.

It is well known that if a single law is to define the variety of groups, it must be of the form $u = v$ where either u or v is just a single variable; thus no generality is sacrificed by assuming the law to be of the form (B.1).

The model will be a suitable cyclic group, written additively, so that $x + y$, $-x$, 0 denote the binary, unary, and nullary operations in it. Put

$$xy\mu = x + y \ ,$$

$$x\iota = -x + c \ ,$$

$$\varepsilon = d \ ,$$

where c, d , and the order p of the group are still to be determined. Then the left-hand side of (B.1) will become

$$w(x, y_1, y_2, \ldots, y_n) = x + kc + ld \ ,$$

where k and l are integers that depend on the number and manner of occurrences of ι and ε in w . Using Lemma 1, k may be assumed to be odd. If $l = 0$, put $c = 0$, $d = 1$, and $p = 2$. Then the law (B.1) will be satisfied, but ε will not be the unit element of the group; in this case ι is inversion. If $l \neq 0$, let p be a prime number greater than $|k|$ and $|l|$, and choose c, d so that

$$kc + ld \equiv 0 \bmod p \ , \quad d \not\equiv 0 \bmod p \ ;$$

for example, $d = 1$. Again the law (B.1) is satisfied, and again ε is not the unit element; in this case ι is not inversion, either. //

References

[1] Richard Hubert Bruck, *A survey of binary systems* (Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, 20. Springer-Verlag, Berlin, Göttingen, Heidelberg, 1958).

https://doi.org/10.1017/S0004972700006912 Published online by Cambridge University Press

[2] Graham Higman and B.H. Neumann, "Groups as groupoids with one law", *Publ. Math. Debrecen* 2 (1952), 215-221.

[3] A. Tarski, "Equational logic and equational theories of algebras", *Contributions to mathematical logic*, 275-288 (Proceedings of the Logic Colloquium, Hannover, 1966. North-Holland, Amsterdam, 1968).

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
PO Box 4,
Canberra, ACT 2600, Australia,

and

Division of Mathematics and Statistics,
Commonwealth Scientific and Industrial Research Organization,
PO Box 1965,
Canberra City, ACT 2601, Australia.