LAWS IN GROUPOIDS DERIVED FROM SEMIGROUPS

Ann Chi Kim

A simple change of the operation in a commutative semigroup leads
to a groupoid. It is shown that it has no finite basis for its
laws.

1. Introduction

Denote by N the set of positive integers, and by N the additive
semigroup of positive integers (so that N is the *carrier* of N).
Introduce a new binary operation μ (written as a right-hand operator) on
N by putting

$$xy\mu = 2x + 3y \ .$$

Then N becomes the carrier of a groupoid, which will be denoted by
$G(2, 3)$, or later by G for short. An obvious generalisation is obtained
if the coefficients $2, 3$ are replaced by some other positive integers,
say a, b ; the resulting groupoid, with the operation μ defined by

$$xy\mu = ax + by \ ,$$

is denoted by $G(a, b)$. Further generalisations suggest themselves: the
semigroup N can be replaced by an arbitrary semigroup S , with carrier
S , and multiplication by a and b by two arbitrary endomorphisms of
S ; thus if "+" is still used for the semigroup operation in S , and if

α, β are two endomorphisms of S, written as left-hand operators, a new operation μ can be defined by

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

defining a groupoid $G(\alpha, \beta)$ with carrier S.

This paper is concerned with one-variable laws in these groupoids, and in fact concentrates on those in $G(2, 3)$, as they are typical of the more general situation. The main result states that the laws of $G(2, 3)$ in any number of variables have no finite basis. Some further generalisations are also mentioned, but not treated in detail.

2. The special case

In this section we consider $G(2, 3)$, though some of the considerations (obviously) have more general application. A "word" w over $G(2, 3)$ is obtained from "variables" $x, y, \ldots, z$ by operating on them with μ, repeatedly: for example

$$w = yx\mu xx\mu y\mu\mu .$$

This can be "evaluated" in N, to give, in an obvious notation,

$$|w| = rx + sy + \ldots + tz$$

with $r, s, \ldots, t \in N$; in the above example,

$$|w| = 36x + 13y .$$

If two words w, w' on evaluation give the same result,

$$|w| = |w'| ,$$

then $w = w'$ is a law in $G(2, 3)$. Thus for example if

$$w' = yxx\mu\mu xy\mu\mu ,$$

then

$$|w'| = 36x + 13y = |w| ,$$

whence

(1) $yx\mu xx\mu y\mu\mu = yxx\mu\mu xy\mu\mu$

is a law in $G(2, 3)$. It is not difficult to verify that this is in fact a law in all $G(a, b)$, and indeed in $G(\alpha, \beta)$ whenever the underlying semigroup S is commutative and the two endomorphisms α and β commute

with each other.

As from here on we shall be mainly concerned with $G(2, 3)$, we write briefly G for this groupoid. If w is a word over G in the single variable x , then $|w| = rx$, with $r \in N$. It is not difficult to compute r ; one can do it by simply replacing x by 1 . For brevity of notation we put

$$\|w\| = r \quad \text{if} \quad |w| = rx \ .$$

The numbers r that thus arise in G are just all the integers of the form $12n + 1$ and $12n + 5$, for $n \geq 0$ – the easy verification is omitted. Again if $\|w\| = \|w'\|$, then $w = w'$ is a law in G . To see when this happens, we first establish a criterion:

LEMMA 1. *If u, v, u', v' are single-variable words in G, then*

(2) $$\|uv\mu\| = \|u'v'\mu\|$$

if, and only if, there is an integer l such that

(3) $$\|u\| - \|u'\| = 12l \quad and \quad \|v'\| - \|v\| = 8l \ .$$

Proof. As

$$\|uv\mu\| = \|u'v'\mu\|$$

if, and only if,

$$2\|u\| + 3\|v\| = 2\|u'\| + 3\|v'\| \ ,$$

(2) is equivalent to

(4) $$2(\|u\|-\|u'\|) = 3(\|v'\|-\|v\|) \ .$$

Since, moreover, the difference between any two numbers of the form $\|w\|$ in G is a multiple of 4 , there are integers m, n such that

(5) $$\|u\| - \|u'\| = 4m \ , \quad \|v'\| - \|v\| = 4n \ .$$

Substituting in (4) gives

(6) $$8m = 12n \ ,$$

whence $m = 3l$ and $n = 2l$ for some integer l . Then (5) and (6) combine to give (3).   //

LEMMA 2. *Let $r \in N$ satisfy*

(7) $$r \equiv 1 \quad or \quad 5 \ (\text{mod } 12) \quad and \quad r \geq 41 \ .$$

Then there are at least two distinct one-variable words w, w' over G with

$$\|w\| = \|w'\| = r$$

(giving the law $w = w'$ in G).

 Proof. Assume the number r satisfies the conditions (7). Then there is at least one single-variable word w over G such that

$$w = uv\mu \text{ , and } \|w\| = r \text{ .}$$

Assume first that $\|v\| \equiv 1 \pmod{12}$. If $\|v\| > 8$, then $\|v\| - 8 \equiv 5 \pmod{12}$ and $\|v\| - 8$ is positive: thus it is itself of the form $\|v'\|$. Also $\|u\| + 12 = \|u'\|$ for some word u' . By Lemma 1 then, with $l = 1$,

(8) $r = \|uv\mu\| = \|u'v'\mu\|$.

If $\|v\| \leq 8$, then $\|v\| = 1$, and we have

$$\|w\| = 2\|u\| + 3\|v\| = 2\|u\| + 3 \geq 41 \text{ ,}$$

whence $\|u\| \geq 19$; but as $\|u\| \equiv 1$ or $5 \pmod{12}$, even $\|u\| \geq 25$. Then there is a word u' such that $\|u'\| = \|u\| - 24$. There is also a v' such that $\|v'\| = \|v\| + 16 \ (= 17)$, and Lemma 1, with $l = -2$, again yields (8). Next assume that $\|v\| \equiv 5 \pmod{12}$. If $\|v\| > 16$, one similarly finds u' and v' with $\|u'\| = \|u\| + 24$ and $\|v'\| = \|v\| - 16$, and applies Lemma 1 with $l = 2$ to obtain (8). If $\|v\| \leq 16$, then $\|v\| = 5$, and

$$\|w\| = 2\|u\| + 3\|v\| = 2\|u\| + 15 \geq 41 \text{ ,}$$

whence $\|u\| \geq 13$. Now choose u' and v' so that $\|u'\| = \|u\| - 12$ and $\|v'\| = \|v\| + 8$, and apply Lemma 1 with $l = -1$, to get (8). Putting $w' = u'v'\mu$ completes the proof of the lemma.   //

 It follows that to each number r that satisfies (7) there is a non-trivial law $w = w'$ in G with $\|w\| = \|w'\| = r$; and it is easily seen that with increasing r there are an increasing number of such laws.

3. Modification of the special groupoid

 In preparation for the proof of the main result in the next section, we now introduce a modification of G . This will depend on a positive

integer k , to be specified later. First we define, for any two numbers $x, y \in N$ with greatest common divisor (x, y) ,

$$x' = \frac{x}{(x,y)} \ , \quad y' = \frac{y}{(x,y)} \ ,$$

so that $(x', y') = 1$. Then we define a new binary operation μ^* on N as carrier as follows:

(9)
$$xy\mu^* = xy\mu \quad \text{if} \quad x'y'\mu \leq k \ ,$$
$$xy\mu^* = x \quad \text{if} \quad x'y'\mu > k \ ;$$

here μ is, of course, the operation of G . The groupoid with carrier N and this binary operation μ^* is denoted by G_k^* . If w is a word over G , the word over G_k^* obtained by replacing μ by μ^* is denoted by w^* . Note that w^* can not, like w , be evaluated in N to give a linear combination of the variables with coefficients in N , because $xy\mu^*$ is itself no longer a single linear combination of x and y . However, if w^* is a word in a single variable x , say, then w^* can be evaluated unambiguously in N , to give

$$|w^*| = r^*x \ ,$$

with $r^* \in N$. Again, if two one-variable words w^*, w'^* over G_k^* give the same result on evaluation:

$$|w^*| = |w'^*| \ ,$$

then $w^* = w'^*$ is a law in G_k^* . Again one readily sees that the $r^* \in N$ that occur here (or, equivalently, that lie in the carrier of the sub-groupoid of G_k^* generated by 1) are all of the form $12n + 1$ or $12n + 5$, with $n \geq 0$ (but now not all of these numbers need occur).

   LEMMA 3. *Let w be a one-variable word over G . If $\|w\| \leq k$, then $|w^*| = |w|$.*

   Proof. We first notice that $x^* = x$. Next let $w = uv\mu$, where u, v are words in x . As

$$\|w\| = 2\|u\| + 3\|v\| \ ,$$

both $\|u\| < \|w\| \leq k$ and $\|v\| < \|w\| \leq k$, so that we may assume that

$$|u^*| = |u| = \|u\|x \quad \text{and} \quad |v^*| = |v| = \|v\|x \ .$$

Now $w^* = u^*v^*\mu^*$, and the first part of the definition (9) of μ^*
applies, so that

$$|w^*| = (2\|u^*\|+3\|v^*\|)x = (2\|u\|+3\|v\|)x = |w| ,$$

as claimed.   //

4. The main results

We now show that the laws of G are not finitely based, in other
words, that they do not follow from any finite number among them.   The
question of what algebras, or classes of algebras, are finitely based has
long been of interest;   see, for example, Tarski's survey [2], pp. 277-278.

LEMMA 4. *Let L be a set of laws of some class C of algebras, and
let L_1 be the set of one-variable specialisations of members of L , that
is to say the set of laws obtained from those in L by putting all
variables equal to a single one, say x . Then every one-variable law of
C that is a consequence of L is also a consequence of L_1 .*

This is the one-variable case of a well known (and almost obvious)
fact applicable to any fixed finite number of variables;   see Neumann [1],
p. 39.   //

THEOREM. *If L is any finite set of laws of G , then there is a
one-variable law of G that is not a consequence of L . Thus the set of
laws of G is not finitely based.*

Proof.   Denote again by L_1 the set of one-variable specialisations
of members of L . By Lemma 4 it suffices to show that there is a law of
G that does not follow from L_1 . To this end we choose the integer
$k \in N$ such that

(10) $k \geq \max\{\|w\| \mid$ there is a law $w = w'$ or $w' = w$ in $L_1\}$,

                    and $k = 36n + 5$ for some integer $n \geq 1$.
With this choice of k we form G_k^* as in the preceding section.   Now if
$w = w'$ is a law of G in L_1 , then Lemma 3 together with the choice of
k guarantees that

$$|w^*| = |w| = |w'| = |w'^*| ,$$

so that $w^* = w'^*$ is also a law of G_k^* . Thus all the laws in L_1 are also, after replacing μ by μ^* , laws of G_k^* ; and so are then all the consequences of L_1 . It remains to exhibit a law of G that is not valid in G_k^* .

Put

$$s = 24n + 1 \ , \quad s' = 36n + 1 \ ,$$

where n is the integer in the definition (10) of k . There are one-variable words, say z and z' , such that, in G ,

$$\|z\| = s \ , \quad \|z'\| = s' \ .$$

Put $w_0 = xz\mu$, $w_0' = z'x\mu$. Then

$$\|w_0\| = 2 + 3s = 72n + 5 = 2s' + 3 = \|w_0'\| \ ,$$

whence $w_0 = w_0'$ is a law in G . We now compute $|w_0^*|$ and $|w_0'^*|$. First notice that as $s < k$ and $s' < k$, we have

$$|z^*| = |z| = sx \ , \quad |z'^*| = |z'| = s'x \ .$$

Now $(1, s) = (s', 1) = 1$, and $1s\mu = s'1\mu = 72n + 5 > k$, so the second part of the definition (9) applies to give

$$|w_0^*| = |x^*z^*\mu^*| \ = |x(sx)\mu^*| \ = x \ ,$$

$$|w_0'^*| = |z'^*x^*\mu^*| = |(s'x)x\mu^*| = s'x \ .$$

As $s' \geq 37$, these two are different, and $w_0^* = w_0'^*$ is not a law in G_k^* . It follows that $w_0 = w_0'$ is not a consequence of L_1 , as required.   //

5.   Some general comments

One can use the same kind of consideration to prove corresponding results for $G(a, b)$ for arbitrary a, b other than $a = b = 1$. The subgroupoid generated by 1 in $G(a, b)$ is never free, as the law (1) is always satisfied; and one easily makes others like it. This answers a question asked by B.H. Neumann. The laws valid simultaneously in all $G(a, b)$, that is to say the laws of the variety generated by all

$G(a, b)$, warrant further study. We only remark that if $w = w'$ is such a
law, then w and w' are words of equal length: this is easily seen by
considering them in (the semigroup) $G(1, 1)$.

The groupoids here considered can be modified in a number of ways.
One such modification uses the following definition of a binary operation
μ :

If $x \neq y$ then $xy\mu = ax + by$, and $xx\mu = cx$, where $a, b, c \in N$.
Denoting the resulting groupoid, on N as carrier, by $G(a, b, c)$, one
sees that $G(a, b, a+b)$ is simply the $G(a, b)$ considered before. These
$G(a, b, c)$ provide further examples of groupoids without finite bases for
their laws. We omit the proof.

References

[1]   Hanna Neumann, "On varieties of groups and their associated near-
            rings", *Math*. Z. **65** (1956), 36-69.

[2]   A. Tarski, "Equational logic and equational theories of algebras",
            Contributions to Mathematical Logic, 274-288 (Proceedings of the
            Logic Colloquium, Hannover, 1966. North-Holland, Amsterdam,
            1968).

Department of Mathematics,
Busan National University,
Pusan,
Korea 607.