BULL. AUSTRAL. MATH. SOC. 08A15
VOL. 13 (1975), 75-83. (20N15)

Equationally complete varieties of generalized groups

W.F. Page

In previous work, Page and Butson [*Algebra Universalis* 3 (1973), 112-126] characterized all equationally complete classes (atoms) of m-semigroups (universal algebras with one m-ary associative operation), and hence m-groups, in the commutative case. The further characterization of the non-commutative m-group atoms was thought to hinge upon a conjecture by Page [PhD thesis, University of Miami, 1973] that a weaker form of commutativity held true. In this paper that conjecture is proved and then used to study the special case $m = 4$. Two additional infinite sets of atoms are thereby determined, although it is not proved that these examples exhaust the remaining atoms for $m = 4$.

1. Notation and preliminaries

For the remainder of this paper, the single m-ary operation on the set A will be denoted by juxtaposition; that is, $x_1x_2 \ldots x_m$ for x_i in A . The associative law is written

$$\left(x_1 \ldots x_m\right)x_{m+1} \ldots x_{2m-1} = x_1 \ldots x_i\left(x_{i+1} \ldots x_{m+i+1}\right)x_{m+i+2} \ldots x_{2m-1}$$

$$\text{for all } x_1, \ldots, x_{2m-1} \text{ in } A \text{ and } i = 1, \ldots, m-1 .$$

The idempotent law is written

$$x \ldots x = x^m = x \text{ for all } x \text{ in } A .$$

The symbol L_m will denote the lattice of equational classes (varieties)

Received 8 April 1975.

of m-semigroups, m an integer. Elements of this lattice will be denoted by script letters, and the terms "atom" and "equationally complete class" will be used interchangeably. Throughout the rest of the paper, the symbol p will stand for an arbitrary prime integer, and congruences will be written in the form $x \equiv y \pmod{t}$. All other notation follows the conventions set forth in [5].

As previously remarked, the commutative atoms of m-semigroups have all been characterized, so that this paper deals exclusively with non-commutative equational classes; that is, those in which the following full abelian law does not hold;

$$x_1 \ldots x_m = x_{\sigma(1)} \ldots x_{\sigma(m)} \quad \text{for all permutations } \sigma \text{ of } \{1, \ldots, m\} .$$

In addition, it was shown [5] that the remaining atoms are actually m-groups in addition to being m-semigroups. The search for equationally complete classes of m-semigroups has therefore been narrowed to special classes of non-abelian m-groups. The reader may consult [2], [3], and [6] for further information on m-groups; although the remaining classes are recognized as m-groups, no use of their formal "group" properties will be made in this paper. The definition of m-group is included here only for the sake of completeness.

DEFINITION. An m-semigroup A is an m-group if, and only if, if in the expression $x_1 \ldots x_m = x_{m+1}$ any m symbols are fixed as elements of A, then the remaining symbol is an element of A, and is uniquely determined.

2. The semi-abelian law

The original definition of semiabelian was given by Dörnte as

$$x_1 x_2 \ldots x_{m-1} x_m = x_m x_2 \ldots x_{m-1} x_1 \quad \text{for } m > 2 .$$

Post, [6], generalized this definition to what he called μ-semi-abelian, as follows

$$x_1 x_2 \ldots x_{\mu-1} x_\mu = x_\mu x_2 \ldots x_{\mu-1} x_1 \quad \text{for } \mu-1 | m-1 .$$

If $\mu = 2$ then this is the usual abelian law. It should be noted also that if $\mu < m$, this expression does not itself define a product, but one merely needs to add the necessary $m - \mu$ elements to each side to evaluate it. Post further defined formal "types" of semi-abelianism in a more general context, where a formal type of semi-abelianism is given by a set of expressions of the form

$$x_1x_2 \dots x_k = x_{\sigma(1)} \dots x_{\sigma(k)} ,$$

where σ is a permutation of $\{1, \dots, k\}$.

Once again, if all the permutation of $\{1, \dots, m\}$ are included, then this is the full abelian law; otherwise it is a weaker form. For each x_i one may compute the displacement of that letter namely $|\sigma(i)-i|$. The following result is due to Post [6].

LEMMA 1 (Post). *Every formal type of semi-abelianism, for* m *fixed, is equivalent to* μ*-semi-abelian with* $\mu - 1 = \gcd(m-1, l_i)$ *, where the* l_i *are the non-zero displacements of the letters in the formal type of semi-abelianism.*

It should be noted here that if an m-group satisfies any formal type of semi-abelianism, then it is at least $(m-1)$-semi-abelian. The above lemma, together with the following lemma due to Page and Butson [5], will yield the proof of the main theorem.

LEMMA 2 (Page and Butson). *Let* V *be a non-commutative idempotent equational class of* L_m . *Then* V *either contains* Z_r, Z_l *, or* PI *, or else it satisfies the identity* $x^{m-1}y = y = yx^{m-1}$ *, in which case* V *is a variety of* m*-groups.*

Since neither Z_r, Z_l nor PI are m-groups, any non-commutative variety of m-groups must necessarily satisfy the identity $x^{m-1}y = y = yx^{m-1}$. Moreover it is also known that any non-idempotent equational class of m-groups will contain an equationally complete class of fully commutative m-groups (this is an adaptation of Theorem 5.1 of [5]). The combination of these results will provide a proof of Theorem 1. If V , a variety of m-groups, is non-idempotent or commutative, then it contains a commutative atom. If it is idempotent and non-commutative then Lemma 2 says that it satisfies $x^{m-1}y = y = yx^{m-1}$. But this last identity is a formal type of semi-abelianism where the displacement of $x = x_1$ is

$m - 1$, and hence V is $(m-1)$-semi-abelian by Lemma 1. The following theorem has been proved.

THEOREM 1. *Every equationally complete* m*-group,* m *arbitrary, is* μ*-semi-abelian, where* $\mu-1 | m-1$.

REMARKS. This theorem is Conjecture 8.1 of [4]. Notice in the special case $m = 2$, this result states that all group atoms are fully abelian.

3. The use of the semi-abelian law in the case $m = 4$

In this section the semi-abelian law is specialized to the case $m = 4$, and is used to help determine two infinite families of equationally complete 4-groups. The remaining work on determining the atoms will depend upon the following theorem, which is stated in its general setting.

THEOREM 2. *Let* V *be an equational class of algebras of type* τ *, and let* I *be the set of identities satisfied by some equational subclass. If a non-trivial relatively free* I*-algebra on* $n \geq 2$ *generators has no non-trivial homomorphic images, then it generates an equationally complete class.*

Let $F_n(I)$ be the relatively free I-algebra on n generators. Because $n \geq 2$, $F_n(I)$ itself is non-trivial. The class generated by I contains an equationally complete class T , and that class contains the algebra $F_n(T)$, which is non-trivial. Because the class generated by I contains the class T , and $F_n(I)$ and $F_n(T)$ are relatively free, any map of the generators of $F_n(I)$ onto the generators of $F_n(T)$ can be extended to a homomorphism. But there were no non-trivial homomorphisms of $F_n(I)$ by hypothesis. Hence, $F_n(I) = F_n(T)$, and $I = T$ is equationally complete.

In the remainder of this section the setting will be the 4-group A , generated by elements a and b , where A satisfies the identities $x^3y = y = yx^3$ and $xyzt = tyzx$ (4-semi-abelian). Thus any word of A is a product of the letters a and b to the 0th, 1st or 2nd power.

LEMMA 3. *Every word in* A *is equal to one of the form* $a \cdot w$ *, where* *the length* $l(w)$ *of the term* w *is congruent to zero modulo three.*

If a word begins with the letter b , replace it by a^3b .

LEMMA 4. *If* $\Theta_{s,t}$ *denotes the smallest congruence relating* s *and* t *, then any congruence in* A *of the form* Θ_{aw_1,aw_2} *is equivalent to one of the form* $\Theta_{a,aw}$.

Multiplying both sides of $aw_1 \equiv aw_2 \pmod{\Theta}$ on the right by w_1^{-1} gives $a \equiv aw_2w_1^{-1} \pmod{\Theta}$ where w_1^{-1} is defined as follows:

if $w_1 = a_1^{i_1} \dots a_n^{i_n}$ then $w_1^{-1} = a_n^{3-i_n} \dots a_1^{3-i_1}$ for $a_i = a$ or b , and $i_k \in \{0, 1, 2\} \pmod 3$.

LEMMA 5. *Every term* w *with* $l(w) \equiv 0 \pmod 3$ *can be written in the form* $\mathrm{a}^j\mathrm{b}^k\mathrm{c}^m$ *, where* $\mathrm{a} = aab$ *,* $\mathrm{b} = aba$ *,* $\mathrm{c} = baa$ *. The exponents* j*,* k *, and* m *are non-negative integers and the terms* a*,* b *, and* c *are triads.*

Because $x^3y = y$, the triads aaa and bbb act as "identity triads" and may be inserted or deleted without changing any product. The remaining triads are $bba = \mathrm{cb}$, $bab = \mathrm{ca}$, and $abb = \mathrm{ba}$. By using the semiabelian law, the order of the triads may be arranged to group all the a's together, all the b's together, and all the c's together.

REMARK. It is now clear that every word in A can be written in the form $a \cdot \mathrm{a}^j\mathrm{b}^k\mathrm{c}^n$. In the remainder of this section this word will be denoted by $a(j, k, n)$.

The term $\mathrm{abc} = \mathrm{cba} = (baa)(aba)(aab)$ acts as an identity. Therefore, since all the triads commute with each other, whenever abc occurs in a product it may be deleted. Hence the following lemma holds.

LEMMA 6. *Every word* $a(j, k, n)$ *is equal to one of the forms* $a(j, k, 0)$ *,* $a(j, 0, k)$ *or* $a(0, j, k)$.

LEMMA 7. *The following congruences are equivalent:* $\Theta_{a,a(j,k,n)}$ *,* $\Theta_{a,a(k,n,j)}$ *, and* $\Theta_{a,a(n,j,k)}$.

https://doi.org/10.1017/S0004972700024266 Published online by Cambridge University Press

Let $a \equiv a(j, k, n) = a\cdot\mathrm{a}^j\mathrm{b}^k\mathrm{c}^n$. Multiply both sides of this congruence by a on the left and a^2 on the right and reassociate triads. This gives a $a\mathrm{c}^j\mathrm{a}^k\mathrm{b}^n = a(k, n, j)$. The equivalence of the remaining congruence is obtained similarly by multiplying both sides by a^2 on the left and a on the right.

LEMMA 8. *If* $n|k$ *, then* $\Theta_{a,a(0,0,n)}$ *implies* $\Theta_{a,a(0,0,k)}$. *If* $n|j$, $n|k$ *, and* $j, k \neq 0$ *, then* $\Theta_{a,a(0,0,n)}$ *implies* $\Theta_{a,a(0,j,k)}$.

To prove the first implication, let $k = sn$ and $a \equiv a\mathrm{c}^n$. Then $a\mathrm{c}^k = a\mathrm{c}^n\mathrm{c}^n \ldots \mathrm{c}^n = (a\mathrm{c}^n)\mathrm{c}^n \ldots \mathrm{c}^n \equiv (a)\mathrm{c}^n \ldots \mathrm{c}^n$, since $a\mathrm{c}^n \equiv a$. Iterating the replacement of the factors $a\mathrm{c}^n$ by a yields, in s steps, $a\mathrm{c}^k \equiv a$. Because $a\mathrm{c}^n \equiv a$ iff $a\mathrm{b}^n \equiv a$ (by Lemma 7), the second part of the theorem can be proved similarly. One iterates the replacement of $a\mathrm{c}^n$ by a and the replacement of $a\mathrm{b}^n$ by a to obtain $a(0, j, k) = a\mathrm{b}^j\mathrm{c}^k \equiv a$.

Now consider A with the additional congruence $\Theta_{a,a(0,0,p)}$. This is the relatively free 4-group on two generators with respect to these relations. This 4-group, denoted by Q_{p^2} , has the following p^2 elements:

$$\begin{array}{lllll} a = & a(0,\ 0,\ 0) & = a(1,\ 1,\ 1) = \ldots = & & a(p,\ p,\ p) \\ & a(0,\ 0,\ 1) & = a(1,\ 1,\ 2) = \ldots = & & a(p,\ p,\ 1) \\ & \vdots & \vdots & & \vdots \\ & a(0,\ p-1,\ p-1) = & \ldots & & = a(p-1,\ p-2,\ p-2)\ . \end{array}$$

Now Q_{p^2} is a relatively free algebra, and for certain values of p it will have no homomorphic images that are non-trivial. To verify this, one must look closely at the congruences on Q_{p^2} . It will be necessary only to consider congruences of the form $\theta_{a,a(0,j,k)}$.

LEMMA 9. *The congruence* $\theta_{a,a(0,s,s+t)}$ *is equivalent to*

https://doi.org/10.1017/S0004972700024266 Published online by Cambridge University Press

$\Theta_{a,a(0,s+t,t)}$.

Let $a \equiv a(0, s, s+t)$, then

$a \equiv a(0, 2s, 2s+2t)$, using Lemma 8,
$\equiv a(0, s, s+t)(0, s, s+t)$, rearranging triads,
$\equiv a(0, s, s+t)(s, s+t, 0)$, Lemma 7,
$\equiv a(s, 2s+t, s+t) \equiv a(0, s+t, t)$, Lemma 6.

LEMMA 10. *The congruence* $\Theta_{a,a(0,j,k)}$ *implies* $\Theta_{a,a(0,0,j^2-jk+k^2)}$.

Let $j > k$. From

(i) $a \equiv a(0, j, k)$

it follows that

(ii) $a \equiv a(0, j-k, j)$ by using Lemma 9.

By Lemma 8, (i) yields $a \equiv a(0, jk, k^2)$, and (ii) yields $a \equiv a(0, (j-k)^2, (j-k)j)$. These two results together give the relation $a \equiv a(0, j^2-jk+k^2, j^2-jk+k^2)$. This last relation and the identity $a \equiv a(j^2-jk+k^2, j^2-jk+k^2, j^2-jk+k^2)$ yield the desired result that $a \equiv a(0, 0, j^2-jk+k^2)$.

LEMMA 11. *In order that the number* p *be represented by the quadratic form* $x^2 - xy + y^2$ *, it is necessary and sufficient that* $p \equiv 1 \pmod 3$ *or* $p = 3$.

Theorem 7, Section 2 [1] gives the necessary and sufficient condition for a form with discriminant D to represent the number p as

$$x^2 \equiv -D \pmod{4p} .$$

But this is true iff p is a quadratic residue mod 3 ; that is, $p \equiv 1 \pmod 3$ or $p = 3$.

If $p \equiv 1 \pmod 3$ or $p = 3$, then there are integers j and k such that $\Theta_{a,a(0,j,k)}$ implies $\Theta_{a,a(0,0,j^2-jk+k^2)} = \Theta_{a,a(0,0,p)}$. Hence there is a non-trivial congruence of Q_{p^2} and, because the order of any m-subgroup divides the order of the m-group, this homomorphic image must

https://doi.org/10.1017/S0004972700024266 Published online by Cambridge University Press

have order p. Then Q_p, the homomorphic image of Q_{p^2}, has no non-trivial homomorphic images because it is of prime order, and will consequently generate an atom.

If $p \equiv 2 \pmod 3$ the representation result used in Lemma 11 will lead to the fact that $(j^2-jk+k^2, p) = 1$ for all j, k relatively prime to p. Then not only will no $\Theta_{a,a(0,j,k)}$ imply $\Theta_{a,a(0,0,p)}$, but instead any $\Theta_{a,a(0,j,k)}$ added to $\Theta_{a,a(0,0,p)}$ will yield the trivial congruence $\Theta_{a,b}$. Then Q_{p^2} has no non-trivial homomorphic images because the identification of any two elements would involve a congruence of the form $\Theta_{a,a(0,j,k)}$ which in turn yields $\Theta_{a,b}$. The following theorem has been established.

THEOREM 3. *The following 4-groups each generate equationally complete classes:*

$$Q_{p^2} = \langle a, b\rangle \text{ with } x^3y = y = yx^3 \text{ and } \Theta_{a,a(0,0,p)}, \text{ if } p \equiv 2 \pmod 3,$$

$$Q_p = \langle a, b\rangle \text{ with } x^3y = y = yx^3 \text{ and } \Theta_{a,a(0,j,k)},$$

$$\text{where } j^2 - jk + k^2 = p, \text{ if } p \equiv 1 \pmod 3) \text{ or } p = 3.$$

REMARK. The variety generated by Q_3 is the previously identified A_3 of [5].

4. Conclusion

Previous work by Page and Butson [5] and Post [6] is used to prove the conjecture (Page [4]) that every equationally complete m-group is at least weakly commutative; that is, μ-semi-abelian, where $\mu-1|m-1$. Use is then made of this new tool in the special case $m = 4$, where two additional infinite families of equationally complete m-groups are determined. Future work in this area may now take advantage of the crucial semi-abelian property, and the fundamental position occupied by the number theoretic lemmas in the case $m = 4$ suggests that elementary properties of congruences may underlie even more the work for $m > 4$.

References

[1] Z.I. Borevich and I.R. Shafarevich, *Number theory* (translated by Newcomb Greenleaf. Pure and Applied Mathematics, 20. Academic Press, New York and London, 1966).

[2] Wilhelm Dörnte, "Untersuchungen über einen verallgemeinerten Gruppenbegriff", *Math. Z.* 29 (1929), 1-19.

[3] J.D. Monk and F.M. Sioson, "On the general theory of m-groups", *Fund. Math.* 72 (1971), 233-244.

[4] William Frank Page, "On the lattice of equational classes of m-semigroups", (PhD thesis, University of Miami, Coral Gables, 1973).

[5] W.F. Page and A.T. Butson, "The lattice of equational classes of m-semigroups", *Algebra Universalis* 3 (1973), 112-126.

[6] Emil L. Post, "Polyadic groups", *Trans. Amer. Math. Soc.* 48 (1940), 208-350.

Department of Mathematics,
University of Miami,
Coral Gables,
Florida,
USA.

https://doi.org/10.1017/S0004972700024266 Published online by Cambridge University Press