On the general theory of m-groups

by

J. D. Monk (Boulder, Colo.) * and F. M. Sioson† **

1. Introduction. The principal objective of this paper is to describe certain properties of m-groups in terms of notions from universal algebra. The concept of an m-group is a straight-forward generalization of the ordinary notion of a (binary) group to one with an arbitrary m-ary operation, where m is any natural number. This was first discovered and studied by Wilhelm Dörnte [2] in 1929. A very extensive memoir on the subject was also published in 1940 by E. L. Post [7]. There have been a number of other mathematicians who have dabbled in the theory. With the increasing interest nowadays among some algebraists in dealing with theories of algebraic systems involving m-ary operations, it is natural to predict that the theory of m-groups should occupy an important place in this developing field. Like their binary counterparts, m-groups possess a very rich and complex theory.

We shall enumerate in this section a number of ways of characterizing the notion of an m-group axiomatically, besides introducing a number of notation conventions. This latter will prove extremely convenient and useful later.

DEFINITION 1.1. An algebraic structure $(A, [\ldots])$ consisting of a set A and an m-ary operation $o\colon A^m \to A$ such that $o(x_1, x_2, \ldots, x_m) = [x_1 x_2 \ldots x_m]$ is called an *m-semigroup* if and only if

$$\big[[x_1 x_2 \ldots x_m] x_{m+1} \ldots x_{2m-1}\big] = \big[x_1 x_2 \ldots x_i [x_{i+1} x_{i+2} \ldots x_{i+m}] \ldots x_{2m-1}\big]$$

for all choices of $i = 1, 2, \ldots, m-1$ and $x_1, x_2, \ldots, x_{2m-1} \in A$.

For simplicity of notation, it will be quite convenient although a little awkward to abbreviate $x_1\ x_2 \ldots x_k$ as x_1^k. In particular, if $x_1 = x_2 = \ldots = x_k = x$, then one may write

$$x_1 x_2 \ldots x_k = (x_1)^k = \ldots = (x_k)^k = x^k.$$

---

* Research supported in part by U. S. National Science Foundation grants GP7387, GP12209.

** Professor Sioson died in his native Phillippines shortly after this article was submitted for publication.

Observe the difference between the notations x_1^k and $(x_1)^k$. On the other hand, if G is an ordinary group, $x \in G$,and n is an integer, $x^{[n]}$ will denote the group-theoretic nth power of x.

We shall also adopt the following inductive definition:

$$x^{\langle 0\rangle} = x\,,$$

$$x^{\langle k+1\rangle} = [x^{\langle k\rangle}x \ldots x] = [x^{\langle k\rangle}x^{m-1}]\,.$$

Observe $\langle 0\rangle = 1$ and $\langle k\rangle = k(m-1)+1$.

The following inductive definition is also frequently useful. For $k > 1$ and elements $x_1, \ldots, x_{km-k+1}$ of an m-semigroup,

$$[x_1^{km-k+1}] = [[x_1^m]x_{m+1}^{km-k+1}]\,.$$

PROPOSITION 1.1. *The following exponential laws hold for any collection of non-negative integers $n_1, \ldots, n_m$ and any element x of an m-semigroup:*

(a) $(x^{\langle n_1\rangle})^{\langle n_2\rangle} = x^{\langle n_1n_2(m-1)+n_1+n_2\rangle}$,

(b) $[x^{\langle n_1\rangle}x^{\langle n_2\rangle} \ldots x^{\langle n_m\rangle}] = x^{\langle n_1+n_2+\ldots+n_m+1\rangle}$.

PROPOSITION 1.2. *If $x_1, \ldots, x_{km-k+s}, y_1, \ldots, y_{hm-h+1}, z_1, \ldots, z_{jm-j+t}$ are elements of an m-semigroup, with $k, j \geqslant 0$, $s+t+1 = m$, and $h > 0$, then*

$$[x_1^{km-k+s}y_1^{hm-h+1}z_1^{jm-j+t}] = [x_1^{km-k+s}[y_1^{hm-h+1}]z_1^{jm-j+t}].$$

DEFINITION 1.3. An $(m-1)$-tuple $(e_1, e_2, \ldots, e_{m-1})$ of elements from an m-semigroup A is called a *left* (*right*) $(m-1)$-*adic identity* if and only if

$$[e_1^{m-1}x] = x$$

($[xe_1^{m-1}] = x$) for all $x \in A$. A *lateral identity* is one which is both a left and right identity. It is simply called an $(m-1)$-*adic identity* if any cyclic permutation of it is a lateral identity.

Any one of the statements in the following theorem is a good definition of an m-group.

THEOREM 1.4. *The following conditions on an m-semigroup $(A, [\ldots])$ are equivalent:*

(1) *For all $a_1, a_2, \ldots, a_m, b \in A$, there exist uniquely $x_1, x_2, \ldots, x_m \in A$ such that*

$$[x_1a_2^m] = b,\ [a_1x_2a_3^m] = b,\ \ldots,\ [a_1^{m-1}x_m] = b;$$

(2_i) *For a fixed $i \neq 1$, m and all $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_m, b \in A$, there exists uniquely an $x_i \in A$ such that $[a_1^{i-1}x_ia_{i+1}^m] = b$;*

(3) *For all $a_1, a_2, \ldots, a_m, b \in A$, there exist uniquely x_1 and x_m in A such that $[x_1a_2^m] = b$ and $[a_1^{m-1}x_m] = b$;*

(4) *For all $a_1, a_2, \ldots, a_{m-2} \in A$, there exist uniquely $a_0, a_{m-1} \in A$ such that $(a_0, a_1, \ldots, a_{m-2})$ and $(a_1, a_2, \ldots, a_{m-1})$ are lateral $(m-1)$-adic identities;*

(5) *For all $a_1, a_2, \ldots a_{m-2}, \in A$, there exists uniquely an element $(a_1, a_2, \ldots a_{m-2})^{-1} \in A$ such that $\big((a_1, a_2, \ldots, a_{m-2})^{-1}, a_1, \ldots, a_{m-2}\big)$ and $\big(a_1, a_2, \ldots, a_{m-2}, (a_1, a_2, \ldots, a_{m-2})^{-1}\big)$ are $(m-1)$-adic lateral idenitities.*

(6_i) *For all $a_1, a_2, \ldots, a_{m-2} \in A$, there exists uniquely an element a_{m-1} such that $(a_{\sigma^i(1)}, a_{\sigma^i(2)}, \ldots, a_{\sigma^i(m-1)})$ is an $(m-1)$-adic lateral identity for a fixed $i \neq 0$, $m-1$ where $\sigma = (12 \ldots m-1)$;*

(7) *For all $a \in A$, there exists uniquely an $\bar a \in A$ such that $(a, a, \ldots, \bar a)$ and $(\bar a, a, \ldots, a)$ are lateral $(m-1)$-adic identities;*

(8_i) *For a fixed $i = 1, 2, \ldots, m-3$ and all $a \in A$, there exists uniquely an $\bar a \in A$ such that $(\overbrace{a \ldots a}^{i}\bar a a \ldots a)$ is a lateral identity.*

Proof. Observe that if for each $i = 2, 3, \ldots, m-1$, $(2_i) \Longleftrightarrow (3)$ then (1)-(3) are equivalent. The proof of the rest of the implications is outlined as follows

$$\begin{array}{ccccccc} (2_i) & \Longleftrightarrow & (3) & \Rightarrow & (4) & \Rightarrow & (5) \\ & & \Downarrow\ \Uparrow & & & & \Downarrow \\ & & (6_i) & \Rightarrow & (8_i) & \Leftarrow & (7) \end{array}$$

$(2_i) \Rightarrow (3)$. Suppose (2_i). For $a_2, \ldots, a_m, b \in A$ and $b_1, \ldots, b_{i-1}, b_{i+1}, \ldots$ $\ldots, b_m \in A$, choose x_1 to be the unique element of A such that

$$[b_1^{i-1}x_1a_2 \ldots a_{m-i}[a_{m-i+1}^m b_{i+1}^m]] = [b_1^{i-1}bb_{i+1}^m]\,.$$

Therefore by (2_i) $[x_1a_2^m] = b$. If, moreover, $[xa_2^m] = [ya_2^m]$ then

$$[b_1^{i-1}xa_2^{m-i}[a_{m-i+1}^m b_{i+1}^m]] = [b_1^{i-1}[xa_2^m]b_{i+1}^m] = [b_1^{i-1}[ya_2^m]b_{i+1}^m]$$
$$= [b_1^{i-1}ya_2^{m-i}[a_{m-i+1}^m b_{i+1}^m]]\,.$$

Whence by (2_i), $x = y$.

The unique solvability of the other equation is shown similarly. By assuming (3) the following lemmas can be proved.

LEMMA 1. *If $[u_1^m] = u_m$ ($[u_1^m] = u_1$), then $[u_1^{m-1}x] = x$ ($[xu_2^m] = x$) for all $x \in A$.*

Proof. We only prove the non-parenthetical remark; the other follows in exactly the same way.

Let $x \in A$ be arbitrary. By (3), there exist $v_2, \ldots, v_m \in A$ such that $[u_mv_2^m] = x$. Hence

$$x = [u_mv_2^m] = [[u_1^m]v_2^m] = [u_1^{m-1}[u_mv_2^m]] = [u_1^{m-1}x]\,.$$

LEMMA 2. *If $(u_1, \ldots, u_{m-1})$ is a left $(m-1)$-adic identity in A, then it is also a right $(m-1)$-adic identity and conversely.*

Proof. Suppose $[u_1^{m-1}x] = x$ for all $x \in A$. Then $[u_1^{m-1}u_1] = u_1$ and hence for any u_0

$$\left[u_0 u_1^{m-2}[u_{m-1}u_1^{m-1}]\right] = \left[u_0[u_1^{m-1}u_1]u_2^{m-1}\right] = [u_0^{m-1}] .$$

Whence by (3) $[u_{m-1}u_1^{m-1}] = u_{m-1}$. By Lemma 1, this implies $[xu_1^{m-1}] = x$ for all $x \in A$.

The proof of the converse is similar.

LEMMA 3. *If $(u_1, \ldots, u_{m-1})$ is an $(m-1)$-adic lateral identity then in fact it is an $(m-1)$-adic identity, i.e., for each i $(u_{\sigma^i(1)}, \ldots, u_{\sigma^i(m-1)})$ is a lateral $(m-1)$-adic identity.*

Proof. We proceed by induction. Suppose $(u_{\sigma^k(1)}, \ldots, u_{\sigma^k(m-1)})$ is a lateral $(m-1)$-adic identity. Then

$$[u_{\sigma^k(1)} \ldots u_{\sigma^k(m-1)} u_{\sigma^k(1)}] = u_{\sigma^k(1)}$$

and hence by Lemma 1,

$$x = [xu_{\sigma^k(2)} \ldots u_{\sigma^k(m-1)} u_{\sigma^k(1)}] = [xu_{\sigma^{k+1}(1)} \ldots u_{\sigma^{k+1}(m-2)} u_{\sigma^{k+1}(m-1)}]$$

for all $x \in A$. Whence $(u_{\sigma^{k+1}(1)}, \ldots, u_{\sigma^{k+1}(m-1)})$ is also a right and hence left $(m-1)$-adic identity, by Lemma 2. The induction is thus complete.

$(3) \Rightarrow (2_i)$ for each i. Let (3) hold. Then there exist $b_i, \ldots, b_{m-1}, c_2, \ldots \ldots, c_i \in A$ such that

$$[b_i^{m-1} a_1^{i-1} a] = a = [aa_{i+1}^m c_2^i] .$$

By the preceding Lemmas 1 and 2, then

$$(b_i, \ldots, b_{m-1}, a_1, \ldots, a_{i-1}) \quad \text{and} \quad (a_{i+1}, \ldots, a_m, c_2, \ldots, c_i)$$

are lateral $(m-1)$-adic identities. By Lemma 3

$$(a_1, \ldots, a_{i-1}, b_i, \ldots, b_{m-1}) \quad \text{and} \quad (c_2, \ldots, c_i, a_{i+1}, \ldots, a_m)$$

are also lateral $(m-1)$-adic identities. To obtain (2_i) choose $x_i = [b_i^{m-1}bc_2^i]$. Then

$$\left[a_1^{i-1}[b_i^{m-1}bc_2^i]a_{i+1}^m\right] = \left[[a_1^{i-1}b_i^{m-1}b]c_2^i a_{i+1}^m\right] = [bc_2^i a_{i+1}^m] = b .$$

If $[a_1^{i-1}xa_{i+1}^m] = [a_1^{i-1}ya_{i+1}^m]$, then

$$x = [xa_{i+1}^m c_2^i] = \left[[b_i^{m-1}a_1^{i-1}x]a_{i+1}^m c_2^i\right] = \left[b_i^{m-1}[a_1^{i-1}xa_{i+1}^m]c_2^i\right]$$
$$= \left[b_i^{m-1}[a_1^{i-1}ya_{i+1}^m]c_2^i\right] = \left[[b_i^{m-1}a_i^{i-1}y]a_{i+1}^m c_2^i\right] = [ya_{i+1}^m c_2^i] = y .$$

The proof of the equivalence of (1)–(3) is now complete.

$(3) \Rightarrow (4)$. Suppose (3) holds and hence Lemmas 1–3. If $a_1, a_2, \ldots, a_{m-1}$ are given, let a_0 be the unique x such that $[xa_1^{m-1}] = a_{m-1}$. Then by Lemmas 1 and 2 $(a_0, a_1, \ldots, a_{m-2})$ is a lateral $(m-1)$-adic identity. By Lemma 3 $(a_1, \ldots, a_{m-2}, a_0)$ is also a lateral $(m-1)$-adic identity thus (4) holds with $a_0 = a_{m-1}$.

$(4) \Rightarrow (5)$. Assuming (4), in this case it suffices to show that if $(a_0, a_1, \ldots, a_{m-2})$ and $(a_1, a_2, \ldots, a_{m-1})$ are lateral $(m-1)$-adic identities then $a_0 = a_{m-1}$. By hypothesis,

$$[a_0^{m-2}x] = x = [xa_0^{m-2}]$$
$$[a_1^{m-1}x] = x = [xa_1^{m-1}] \quad \text{for all } x \in A .$$

Taking $x = a_{m-1}$ in the first and $x = a_0$ in the second, then $a_{m-1} = [a_0^{m-1}] = a_0$.

$(5) \Rightarrow (7)$. Suppose (5) holds. Then for $a_1 = a_2 = \ldots = a_{m-2} = a$, there exists uniquely an $\bar{a} \in A$ such that

$$(\bar{a}, a, \ldots, a) \quad \text{and} \quad (a, a, \ldots, \bar{a})$$

are both lateral $(m-1)$-adic identities.

$(3) \Rightarrow (6_i)$. Thus assuming (3) we have the validity of Lemmas 1–3. Let $a_1, a_2, \ldots, a_{m-2} \in A$. Then for any other $b \in A$ let a_{m-1} be the unique x such that

$$[xa_1^{m-2}b] = b \quad \text{or} \quad [a_{m-1}a_1^{m-2}b] = b .$$

By Lemma 1, then $[a_{m-1}a_1^{m-2}x] = x$ for all $x \in A$. Whence $(a_{m-1}, a_1, \ldots, a_{m-2})$ is a lateral $(m-1)$-adic identity and hence by Lemma 3 so is

$$(a_{\sigma^i(1)}, a_{\sigma^i(2)}, \ldots, a_{\sigma^i(m-1)}) \quad \text{for all } i = 1, \ldots, m-2 .$$

$(6_i) \Rightarrow (8_i)$ for the same $i = 1, \ldots, m-2$ is clear.

$(7) \Rightarrow (8_i)$. Assume (7). The following lemmas then follow:

LEMMA 4. *For all $k = 0, 1, \ldots, m-1$ we have*

$$[a^k \bar{a} a^{m-k-1}] = a .$$

Proof by induction. Clearly from the hypothesis

$$[\bar{a}a^{m-1}] = [a\bar{a}a^{m-2}] = a = [a^{m-1}\bar{a}] = [a^{m-2}\bar{a}a] .$$

Suppose $[a^{k-1}\bar{a}a^{m-k}] = a$. Then

$$a = [a^{k-1}\bar{a}a^{m-k}] = \left[a^{k-1}\bar{a}[a^{m-1}\bar{a}]a^{m-k-1}\right]$$
$$= \left[[a^{k-1}\bar{a}a^{m-k}]a^{k-1}\bar{a}a^{m-k-1}\right] = [a^k\bar{a}a^{m-k-1}] .$$

The induction is thus complete.

LEMMA 5. *For all $k = 0, 1, \ldots, m-1$, we have $(\overbrace{a, \ldots, a}^{k}, \bar{a}, a, \ldots, a)$ is a lateral $(m-1)$-adic identity.*

Proof.

$$[a^k\bar{a}a^{m-k-2}x] = \big[a^k\bar{a}a^{m-k-2}[a^{m-2}\bar{a}x]\big]$$
$$= \big[[a^k\bar{a}a^{m-k-1}]a^{m-3}\bar{a}x\big] = [a^{m-2}\bar{a}x] = x \quad \text{for all } x \in A.$$

Similarly,

$$[xa^k\bar{a}a^{m-k-2}] = \big[[x\bar{a}a^{m-2}]a^k\bar{a}a^{m-k-2}\big]$$
$$= \big[x\bar{a}a^{m-3}[a^{k+1}\bar{a}a^{m-k-2}]\big] = [x\bar{a}a^{m-2}] = x \quad \text{for all } x \in A.$$

To show uniqueness, suppose also (a^iba^{m-i-2}) is a lateral identity. Then for any $x \in A$,

$$[xa^{m-2}b] = \big[xa^{m-2}[ba^{m-2}\bar{a}]\big] = \big[xa^{m-2-i}[a^iba^{m-i-1}]a^{i-1}\bar{a}\big]$$
$$= [xa^{m-2}\bar{a}] = x.$$

Similarly it is shown that $(a^{m-2}b)$ is a left identity, and (ba^{m-2}) is a lateral identity. Hence by (7) $\bar{a} = b$.

Whence (8_i) holds.

$(8_i) \Rightarrow (3)$. Assume that (8_i) holds and let

$$x_1 = [b(a_m)^i\bar{a}_m(a_m)^{m-i-3}(a_{m-1})^i\bar{a}_{m-1}(a_{m-1})^{m-i-3} \ldots (a_2)^i\bar{a}_2(a_2)^{m-i-3}],$$
$$x_m = [(a_{m-1})^{i-1}\bar{a}_{m-1}(a_{m-1})^{m-i-2}(a_{m-2})^{i-1}\bar{a}_{m-2}(a_{m-2})^{m-i-2} \ldots$$
$$\ldots (a_1)^{i-1}\bar{a}_1(a_1)^{m-i-2}b]$$

then

$$[x_1a_2^m] = [b(a_m)^i\bar{a}_m(a_m)^{m-i-3} \ldots (a_3)^i\bar{a}_3(a_3)^{m-i-3}(a_2)^i(\bar{a}_2)a_2^{m-i-3}a_2a_3 \ldots a_m]$$
$$= \big[b(a_m)^i\bar{a}_m(a_m)^{m-i-3} \ldots (a_3)^i\bar{a}_3(a_3)^{m-i-3}[(a_2)^i\bar{a}_2(a_2)^{m-i-2}a_3]a_4 \ldots a_m\big]$$
$$= \big[b(a_m)^i\bar{a}_m(a_m)^{m-i-3} \ldots [(a_3)^i\bar{a}_3(a_3)^{m-i-2}a_4] \ldots a_m\big]$$
$$= \ldots = [b(a_m)^i\bar{a}_m(a_m)^{m-i-2}] = b.$$

Similarly,

$$[a_1^{m-1}x_m]$$
$$= [a_1^{m-1}(a_{m-1})^{i-1}\bar{a}_{m-1}(a_{m-1})^{m-i-2} \ldots (a_2)^{i-1}\bar{a}_2(a_2)^{m-i-2}(a_1)^{i-1}\bar{a}_1(a_1)^{m-i-2}b]$$
$$= \big[a_1^{m-3}[a_{m-2}(a_{m-1})^i\bar{a}_{m-1}(a_{m-1})^{m-i-2}] \ldots (a_1)^{i-1}\bar{a}_1(a_1)^{m-i-2}b\big]$$
$$= \ldots = \big[[a_1(a_2)^i\bar{a}_2(a_2)^{m-i-2}](a_1)^{i-1}\bar{a}_1(a_1)^{m-i-2}b\big] = [(a_1)^i\bar{a}_1(a_1)^{m-i-2}b] = b.$$

Suppose $[xa_2^m] = [ya_2^m]$. Then

$$[xa_2^{m-1}(a_m)^i\bar{a}_m(a_m)^{m-i-2} \ldots (a_2)^{i-1}\bar{a}_2(a_2)^{m-i-2}]$$
$$= [ya_2^{m-1}(a_m)^i\bar{a}_m(a_m)^{m-i-2} \ldots (a_2)^{i-1}\bar{a}_2(a_2)^{m-i-2}],$$

so that

$$x = [x(a_2)^i\bar{a}_2(a_2)^{m-i-2}] = [y(a_2)^i\bar{a}_2(a_2)^{m-i-2}] = y.$$

Similarly, if $[a_1^{m-1}x] = [a_1^{m-1}y]$, then $x = y$. The proof of the theorem is now complete.

We will make use below of Post's coset theorem, in the following form (see Bruck [1]): For any m-group A there is a group $G \supseteq A$ such that A generates G and $[x_1 \ldots x_m] = x_1 \cdot \ldots \cdot x_m$ for all $x_1, \ldots, x_m \in A$. If G is the covering group explicitly constructed in Post [7] or Bruck [1] we call G a *free covering group* of A.

2. Algebraic theory. For information on universal algebra consult [4] or Chapter 0 of [5].

THEOREM 2.1. *The class $\mathcal{A}$ of all m-groups is a variety, i.e., is closed under homomorphisms, direct products, and subalgebras.*

Proof. This is clear if one defines an m-group as an m-semigroup $(A, [\ldots], {}^-)$ such that

$$[\bar{x}x^{m-2}y] = [y\bar{x}x^{m-2}] = y = [x^{m-2}\bar{x}y] = [yx^{m-2}\bar{x}]$$

for all x and y in A or an m-semigroup $(A, [\ldots], (\ldots)^{-1})$ such that

$$[(x_1, x_2, \ldots, x_{m-2})^{-1}x_1^{m-2}y] = [y(x_1, x_2, \ldots, x_{m-2})^{-1}x_1^{m-2}] = y$$
$$= [x_1^{m-2}(x_1, x_2, \ldots, x_{m-2})^{-1}y] = [yx_1^{m-2}(x_1, x_2, \ldots, x_{m-2})^{-1}].$$

Observe that in the first instance we have an m-ary and a unary operation, while in the 2nd we have an m-ary and an $(m-2)$-ary operation.

Note that the uniqueness condition can be omitted in Theorem 1.4 (7). Indeed, suppose that $a^{m-2}b$, ba^{m-2}, $a^{m-2}c$, and ca^{m-2} are all lateral $(m-1)$-adic identities. Then

$$b = [ba^{m-2}c] \qquad (\text{since } a^{m-2}c \text{ is an identity})$$
$$= c \qquad (\text{since } ba^{m-2} \text{ is an identity}).$$

By this remark we see that the notions of homomorphism and congruence relation are independent of whether we consider m-groups as structures of the form $(A, [\ldots])$ or $(A, [\ldots], {}^-)$.

THEOREM 2.2. *The lattice of congruence relations in an m-group is modular, in fact congruences are permutable.*

Proof. Consider the word $[xy^{m-3}\bar{y}z]$. Suppose $(x, z) \in \Theta \circ \Phi$ so that $(x, y) \in \Theta$ and $(y, z) \in \Phi$ for some y. Then

$$(x, [xy^{m-3}\bar{y}z]) = ([xy^{m-3}\bar{y}y], [xy^{m-3}\bar{y}z]) \in \Phi,$$
$$([xy^{m-3}\bar{y}z], [x^{m-2}\bar{x}z]) = ([xy^{m-3}\bar{y}z], z) \in \Theta$$

whence $(x, z) \in \Phi \circ \Theta$ and conversely, and $\Theta \circ \Phi = \Phi \circ \Theta$ for any pair of congruence Θ and Φ.

THEOREM 2.3. *The class of all elementary translations in any m-group $(A, [\ldots])$ forms a transitive group.*

Proof. Observe that a basic translation $t(x) = [a_1^{i-1} x a_{i+1}^m]$ is always invertible. Its inverse is $t^{-1}(x) = [b_i^{m-1} x c_2^i]$ where $(b_i, \ldots, b_{m-1}, a_1, \ldots, a_{i-1})$ and $(a_{i+1}, \ldots, a_m, c_2, \ldots, c_i)$ are $(m-1)$-adic identities. An elementary translation is a composition of basic translations and hence is always invertible. Thus they form a group. Transitivity is clear, for, if $a, b \in A$ are arbitrary, then

$$b = [a_1^{i-1} a a_{i+1}^{m-1} x]$$

possesses the unique solution $x = a_m$ and the translation

$$t(x) = [a_1^{i-1} x a_{i+1}^m]$$

gives us $t(a) = b$.

Recall that if $\mathfrak{T}$ is the set of all elementary translations of an algebraic system an equivalence relation Θ is a congruence relation iff $(x, y) \in \Theta$ implies $(t(x), t(y)) \in \Theta$ for all $t \in \mathfrak{T}$.

DEFINITION 2.4. For any $z \in A$ (an m-group), a *z-ideal* is a set of the form z/Θ for some congruence relation Θ in A.

THEOREM 2.5. *The z-ideals of any m-group function properly, i.e., if $z/\Theta = z/\Phi$, then $\Theta = \Phi$.*

Proof. Suppose $z/\Theta = z/\Phi$ and let $(x, y) \in \Theta$. Then for $t \in \mathfrak{T}$ such that $t(x) = z$, we have

$$(t(x), t(y)) = (z, t(y)) \in \Theta \quad \text{or} \quad t(y) \in z/\Theta = z/\Phi .$$

In other words $(z, t(y)) \in \Phi$ and hence $(t^{-1}(z), t^{-1}t(y)) = (x, y) \in \Phi$, whence $\Theta \subseteq \Phi$. Similarly $\Phi \subseteq \Theta$ and therefore $\Theta = \Phi$.

The notion of z-ideal can be characterized as follows without reference to the notion of a congruence relation.

THEOREM 2.6. *Let A be an m-group and let $z \in A$. Then the following two conditions are equivalent:*

(i) *I is a z-ideal;*

(ii) (a) *$z \in I$,*

(b) *if $x, y \in I$ then $[x\bar{z}z^{m-3}y] \in I$,*

(c) *if $x, y \in A$ and $[x\bar{y}y^{m-3}z] \in I$, then $[y\bar{x}x^{m-3}z] \in I$,*

(d) *if $x_1, \ldots, x_{m-1} \in A$ and $[x_1^{m-1}z] \in I$, and if $w \in A$, then $[[wx_1^{m-1}]\bar{w}w^{m-3}z] \in I$.*

Remark. If $m = 3$ then in (ii) the factors z^{m-3}, y^{m-3}, x^{m-3}, w^{m-3} are to be omitted. Similarly in the proof below.

Proof. (i) $\Rightarrow$ (ii). Assume that $I = z/\Phi$, Φ a congruence relation on A. (ii) (a) is obvious. As to (ii) (b), if $x, y \in I$ then $x\Phi z$, $y\Phi z$, so

$$[x\bar{z}z^{m-3}y]\Phi[z\bar{z}z^{m-2}] = z$$

hence $[x\bar{z}z^{m-3}y] \in I$. Now assume the hypothesis of (ii) (c). Then

$$x = [x\bar{y}y^{m-2}] = \big[x\bar{y}y^{m-3}[z\bar{z}z^{m-3}y]\big]$$
$$= \big[[x\bar{y}y^{m-3}z]\bar{z}z^{m-3}y\big]\Phi[z\bar{z}z^{m-3}y] = y .$$

Thus $x\Phi y$. Hence

$$[y\bar{x}x^{m-3}z]\Phi[x\bar{x}x^{m-3}z] = z$$

and $[y\bar{x}x^{m-3}z] \in I$, as desired. Next, assume the hypothesis of (ii) (d). Then

$$\big[[wx_1^{m-1}]\bar{w}w^{m-3}z\big] = \big[[wx_1^{m-1}][z^{m-2}\bar{z}\bar{w}]w^{m-3}z\big] = \big[w[x_1^{m-1}[z^{m-2}\bar{z}\bar{w}]]w^{m-3}z\big]$$
$$= \big[w[[x_1^{m-1}z]z^{m-3}\bar{z}\bar{w}]w^{m-3}z\big]\,\Phi\big[w[z^{m-2}\bar{z}\bar{w}]w^{m-2}z\big]$$
$$= [w\bar{w}w^{m-3}z] = z$$

hence $\big[[wx_1^{m-1}]\bar{w}w^{m-3}z\big] \in I$, as desired.

(ii) $\Rightarrow$ (i). Assume (ii). Let Φ be the set of all pairs $(x, y) \in A \times A$ such that $[x\bar{y}y^{m-3}z] \in I$. By (ii) (a), Φ is reflexive on A; and (ii) (c) says that Φ is symmetric. Now assume that $(u, v), (v, w) \in \Phi$. Thus $[u\bar{v}v^{m-3}z]$, $[v\bar{w}w^{m-3}z] \in I$. Hence

$$[u\bar{w}w^{m-3}z] = \big[[u\,\bar{v}v^{m-2}]\,\bar{w}w^{m-3}z\big] = \big[[\overline{u\,\bar{v}v}^{m-3}[z\bar{z}z^{m-3}v]]\,\overline{\bar{w}w}^{m-3}z\big]$$
$$= \big[[[u\,\bar{v}v^{m-3}z]\bar{z}z^{m-3}v]\,\bar{w}w^{m-3}z\big] = \big[[u\,\bar{v}v^{m-3}z]\bar{z}z^{m-3}[v\,\bar{w}w^{m-3}z]\big] \in I$$

by (ii) (b). Hence $(u, w) \in \Phi$, so Φ is transitive. Next, Φ preserves $[\ldots]$. For, suppose that $(x_1, y_1), \ldots, (x_m, y_m) \in \Phi$. Thus for each $i = 1, \ldots, m$ we have $[x_i\bar{y}_i(y_i)^{m-3}z] \in I$.

LEMMA. *For $i = 0, \ldots, m-1$ we have*

$$[x_{m-i}^m\bar{y}_m(y_m)^{m-3}\bar{y}_{m-1}(y_{m-1})^{m-3} \ldots \bar{y}_{m-i}(y_{m-i})^{m-3}z] \in I .$$

Proof. By induction on i. The case $i = 0$ is immediate. Suppose true for i, $i < m-1$. Then by (ii) (d),

$$(1) \qquad [x_{m-i-1}^m\bar{y}_m(y_m)^{m-3}\bar{y}_{m-1}(y_{m-1})^{m-3} \ldots$$
$$\ldots \bar{y}_{m-i}(y_{m-i})^{m-3}\bar{x}_{m-i-1}(\bar{x}_{m-i-1})^{m-3}z] \in I.$$

Applying (ii) (b) to (1) and to $[x_{m-i-1}\bar{y}_{m-i-1}(y_{m-i-1})^{m-3}z] \in I$ we obtain

$$[x_{m-i-1}^m\bar{y}_m(y_m)^{m-3}\bar{y}_{m-1}(y_{m-1})^{m-3} \ldots$$
$$\ldots \bar{y}_{m-i}(y_{m-i})^{m-3}\bar{x}_{m-i-1}(x_{m-i-1})^{m-3}z\bar{z}z^{m-3}x_{m-i-1}\bar{y}_{m-i-1}(y_{m-i-1})^{m-3}z] \in I$$

from which the lemma for $i+1$ easily follows, using the fact that both $z\bar{z}z^{m-3}$ and $\bar{x}_{m-i-1}(x_{m-i-1})^{m-2}$ are identities. This completes the proof of the lemma.

At this point it is convenient to work with a covering group $(G, \cdot)$ of $(A, [\ldots])$. Note that $\bar{u} = u^{[2-m]}$ for any $u \in A$ and hence $\bar{u} \cdot u^{[m-3]} = u^{[-1]}$. The lemma for $i = m-1$ then gives

$$x_1 \cdot \ldots \cdot x_m \cdot y_m^{[-1]} \cdot y_{m-1}^{[-1]} \cdot \ldots \cdot y_1^{[-1]} \cdot z \in I .$$

Since $[y_1 \cdot \ldots \cdot y_m]^{[-1]} = y_m^{[-1]} \cdot \ldots \cdot y_1^{[-1]}$, we get

$$\begin{aligned} x_1 \cdot \ldots \cdot x_m \cdot y_m^{[-1]} \cdot \ldots \cdot y_1^{[-1]} \cdot z &= [x_1 \ldots x_m] \cdot [y_1 \ldots y_m]^{[-1]} \cdot z \\ &= [x_1 \ldots x_m] \cdot \overline{[y_1 \ldots y_m]} \cdot [y_1 \ldots y_m]^{[m-3]} \cdot z \\ &= \left[[x_1 \ldots x_m] \overline{[y_1 \ldots y_m]} [y_1 \ldots y_m]^{m-3} z\right] . \end{aligned}$$

Hence $[x_1 \ldots x_m] \Phi [y_1 \ldots y_m]$. Thus Φ is a congruence relation on A. It remains only to show that $I = z/\Phi$. If $x \in I$, then $x = [x\bar{z}z^{m-3}z] \in I$, so $x \Phi z$ and $x \in z/\Phi$; the converse is similar. This completes the proof of Theorem 2.6.

In the theory of m-groups the z-ideals serve the same purposes as normal subgroups of groups. In fact, normal subgroups are simply e-ideals, e the identity of the group. However, in m-groups there appears in general to be no natural choice for z.

Theorem 2.7. *Let A be an m-group expressed by Post's coset theorem in the form $A = z \cdot N$, N a normal subgroup of a group G. Let L_1 be the lattice of all subgroups of N invariant under all inner automorphisms $x \mapsto z \cdot w \cdot x \cdot w^{[-1]} \cdot z^{[-1]}$ with $w \in N$. Then L_1 is isomorphic to the lattice L_2 of congruence relations on A.*

Proof. By Theorem 2.5 we know that L_2 is isomorphic to the lattice L_3 of z-ideals of A, so it suffices to show that $L_1 \cong L_3$.

For any z-ideal I of A let $FI = \{x \in N\colon\ z \cdot x \in I\}$. Clearly $e \in FI$. Suppose $x, y \in FI$; we show that $x \cdot y \in FI$. Now $z \cdot x, z \cdot y \in I$. By 2.6 (ii) (b), $[(z \cdot x)\bar{z}z^{m-3}(z \cdot y)] \in I$. Hence $z \cdot x \cdot z^{[-1]} \cdot z \cdot y \in I$, i.e., $z \cdot x \cdot y \in I$; $x \cdot y \in FI$. Next, FI is closed under ${}^{[-1]}$. For, suppose $x \in FI$, thus $z \cdot x \in I$. Now $z \cdot x = [(z \cdot x)\bar{z}z^{m-3}z]$, so by 2.6 (ii) (c), $[z\overline{z \cdot x}(z \cdot x)^{m-3}z] \in I$, i.e., $z \cdot (z \cdot x)^{[-1]} \cdot z \in I$, hence $z \cdot x^{[-1]} \in I$ and $x^{[-1]} \in FI$. Next, let $w \in N$; we show that FI is closed under the inner automorphism associated with $z \cdot w$. Let $x \in FI$, thus again $z \cdot x \in I$. Now since N is normal in G, $z \cdot w \cdot z^{[-1]} \in N$, and $z^{[2]} \cdot w \cdot z^{[-1]} \in A$. Furthermore, $z \cdot x = [(z \cdot x)\bar{z}z^{m-3}z] \in I$. Hence, by 2.6 (ii)(d), with $t = z^{[2]} \cdot w \cdot z^{[-1]}$,

$$\left[[t(z \cdot x)\bar{z}z^{m-3}]\bar{t}t^{m-3}z\right] \in I .$$

However,

$$\begin{aligned} \left[[t(z \cdot x)\bar{z}z^{m-3}]\bar{t}t^{m-3}z\right] &= z^{[2]} \cdot w \cdot z^{[-1]} \cdot z \cdot x \cdot z^{[-1]} \cdot z \cdot w^{[-1]} \cdot z^{[-2]} \cdot z \\ &= z^{[2]} \cdot w \cdot x \cdot w^{[-1]} \cdot z^{[-1]}. \end{aligned}$$

It follows that $z \cdot w \cdot x \cdot w^{[-1]} \cdot z^{[-1]} \in FI$, as desired. Thus F maps L_3 into L_1. Clearly F preserves order. To finish the proof it suffices to construct the order-preserving inverse of F.

For any $P \in L_1$ let $GP = \{x \in A\colon\ z^{[-1]} \cdot x \in P\}$. Clearly all we need to do is to show that GP is a z-ideal. Condition 2.6 (ii) (a) is obvious. Now suppose $x, y \in GP$; thus $z^{[-1]} \cdot x \in P$ and $z^{[-1]} \cdot y \in P$, so $z^{[-1]} \cdot x \cdot z^{[-1]} \cdot y \in P$. Hence $[x\bar{z}z^{m-3}y] \in GP$, so 2.6 (ii) (b) holds. Next suppose $x, y \in A$ and $[x\bar{y}y^{m-3}z] \in GP$. Thus $z^{[-1]} \cdot x \cdot y^{[-1]} \cdot z \in P$, and consequently $z^{[-1]} \cdot y \cdot x^{[-1]} \cdot z \in P$, hence $[y\bar{x}x^{m-3}z] \in GP$ and 2.6 (ii) (c) holds. Finally, suppose $x_1, \ldots, x_{m-1}, w \in A$ and $[x_1^{m-1}z] \in GP$. Thus $z^{[-1]} \cdot x_1 \cdot \ldots \cdot x_{m-1} \cdot z \in P$. Now $w \in A$ implies that $z^{[-1]} \cdot w \in N$; N being normal in G, $z^{[-2]} \cdot w \cdot z \in N$. Since P is closed under the inner automorphism associated with $z^{[-1]} \cdot w \cdot z$, we get

$$z^{[-1]} \cdot \left[[wx_1^{m-1}]\bar{w}w^{m-3}z\right] = z^{[-1]} \cdot w \cdot z \cdot z^{[-1]} \cdot x_1 \cdot \ldots \cdot x_{m-1} \cdot z \cdot z^{[-1]} \cdot w^{[-1]} \cdot z \in P.$$

Hence $\left[[wx_1^{m-1}]\bar{w}w^{m-3}z\right] \in gP$. Thus 2.6 (ii) (d) holds. This completes the proof of 2.7.

Theorem 2.8. *Any two m-groups A and B can be isomorphically embedded in a third m-group C.*

Proof. Let A and B have covering groups G, H respectively, and let C be the m-group reduct of the group $G \times H$. By symmetry we show only that A can be embedded in C. For any $x \in A$ let $Fx = (x, e)$, e the identity of H. Then for any $x_1, \ldots, x_m \in A$,

$$\begin{aligned} F[x_1^m] &= ([x_1^m], e) = (x_1 \cdot \ldots \cdot x_m, e) = (x_1, e) \cdot \ldots \cdot (x_m, e) \\ &= [(x_1, e) \ldots (x_m, e)] = [Fx_1 \ldots Fx_m] . \end{aligned}$$

Clearly F is one-one, so this completes the proof.

It follows that free products of m-groups exist. Note that the above theorem and proof obviously extend to the case of an infinite number of m-groups.

Theorem 2.9. *Let an m-group A be covered by a group G. If $f\colon G \to \prod_{i \in I} G_i$ is an isomorphism between G and a subdirect product of groups G_i, then $f|A\colon A \to \prod_{i \in I} A_i$ is an isomorphism between A and a subdirect product of certain m-groups A_i covered by G_i.*

Proof. Let $A_i = pr_i^* f^* A$, i.e., the image of A under the homomorphism $pr_i \circ f$, where pr_i is the projection into the ith coordinate.

Thus A_i is an m-group. Since A generates G, A_i generates $G_i = pr_i^* f^* G$. For any $i \in I$ and $a_1, \ldots, a_m \in A$ we have

$$[(fa_1)_i \ldots (fa_m)_i] = (f[a_1 \ldots a_m])_i = \big(f(a_1 \cdot \ldots \cdot a_m)\big)_i$$
$$= (fa_1 \cdot \ldots \cdot fa_m)_i = (fa_1)_i \cdot \ldots \cdot (fa_m)_i \, .$$

It follows that for any $i \in I$ and any $x_1, \ldots, x_m \in A_i$ we have

$$[x_1 \ldots x_m] = x_1 \cdot \ldots \cdot x_m \, .$$

Thus G_i covers A_i, as desired. This completes the proof.

THEOREM 2.10. *Let $X \subseteq A$ generate an m-group A freely covered by a group G. Then A is free on X if and only if G is free on X.*

Proof. First suppose that G is free on X. Consider any m-group B and any map $f\colon X \to B$. Let B be covered by a group H. Then there exists a homomorphism $g\colon G \to H$ such that $f \subseteq g$. Clearly $g|A$ is a homomorphism from A into the m-group reduct C of H. Since $g^* X \subseteq B$ and X generates A, $g^* A \subseteq B$. Thus $g|A$ is a homomorphism from A into B, as desired. [Note that in this part of the proof we did not use the assumption that G *freely* covers A.]

Conversely, suppose A is free on X. Let H be any group, and suppose that $f\colon X \to H$. Let B be the m-group reduct of H. Then there exists a homomorphism $g\colon A \to B$ with $f \subseteq g$. Define $g^+\colon A \to G \times H$ by $g^+ a = (a, ga)$ for all $a \in A$. Clearly g^+ is an isomorphism from A into the m-group reduct of $G \times H$. By the well-known replacement theorem of universal algebra there is a group $K \supseteq A$ with an isomorphism h of K onto $G \times H$ such that $g^+ \subseteq h$. Let K' be the subgroup of K generated by A. It is easily verified that K' covers A. Since G freely covers A, it follows that there is a homomorphism $k\colon G \to K'$ which is the identity on A. Then $pr_1 \circ h \circ k$ is a homomorphism from G into H which extends f, as desired.

References

[1] R. H. Bruck, *A survey of binary systems*, 1966, pp. viii+185.
[2] W. Dörnte, *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Zeit. 29 (1928), pp. 1–19.
[3] Π. Глускин, *Позиционные оперативы*, Mat. Sb. 68 (1965), pp. 444–472.
[4] G. Grätzer, *Universal algebra*, 1968, pp. xvi+368.
[5] L. Henkin, D. Monk and A. Tarski, *Cylindric algebras*, Part I, North-Holland, 1971, p. 508.
[6] D. Monk and F. Sioson, *m-semigroups, semigroups, and function representations*, Fund. Math. 59 (1966), pp. 233–241.
[7] E. Post, *Polyadic groups*, Trans. Amer. Math. Soc. 48 (1940), pp. 208–350.
[8] R. Sikorski, *Products of abstract algebras*, Fund. Math. 39 (1952), pp. 211–228.

Reçu par la Rédaction le 2. 8. 1969

Nichtaxiomatisierbarkeit von Satzmengen durch Ausdrücke spezieller Gestalt

von

Kurt Hauschild (Berlin)

In der vorliegenden Arbeit geht es u.a. um folgende Fragen: (1) Ist die Menge der in einer Algebra $\mathfrak{A}$ gültigen (elementaren) Sätze durch Aussagen universell beschränkter Tiefe axiomatisierbar? (2) Gibt es in $\mathfrak{A}$ eine (elementar) definierbare Funktion, die sich von allen durch Ausdrücke einer universell beschränkten Tiefe (elementar) definierbaren Funktionen fast überall unterscheidet? Für den Fall, daß in $\mathfrak{A}$ eine Wohlordnung definierbar ist und für jedes Element ein Term zur Verfügung steht, wird gezeigt, dass (1) verneint werden muss, sobald (2) zu bejahen ist. Dieses Resultat läßt sich noch wesentlich verschärfen. Einerseits braucht in $\mathfrak{A}$ nur ein Teil des elementaren Wohlordnungsschemas zu gelten, andererseits kann man anstelle der Ausdrücke universell beschränkter Tiefe auch andere "hereditäre" Ausdrucksmengen betrachten. Dabei sind hereditäre Ausdrucksmengen im wesentlichen solche, die gegenüber der Bildung von Teilausdrücken abgeschlossen sind.

Die Terminologie ist die in der Modelltheorie allgemein übliche, so dass ich auf diesbezügliche Erörterungen glaube verzichten zu dürfen. Nur folgendes sei bemerkt: Variable werden grundsätzlich mit kleinen normalen lateinischen Buchstaben notiert $(x, y, z, \ldots)$. Elemente mit kleinen fettgedruckten lateinischen Buchstaben $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \ldots)$, Ausdrücke mit kleinen griechischen Buchstaben $(\varphi, \psi, \ldots)$; $\mathfrak{A} \models \varphi(\boldsymbol{x})$ soll bedeuten, daß $\varphi(x)$ in der Algebra $\mathfrak{A}$ gültig wird bei jeder Belegung, die Variable x mit dem Element $\boldsymbol{x}$ belegt.

Es sei L eine elementare Sprache (mit Identität). $Y \subseteq L$ sei eine zunächst beliebige Menge von Ausdrücken. Wir wollen voraussetzen, daß L ein zweistelliges Relationszeichen $\leqslant$ enthält. $\mathfrak{A}$ sei eine Interpretation von L, für die folgendes gilt:

(1) $$\mathfrak{A} \models \forall x\, x \leqslant x \wedge \forall x \forall y \forall z (x \leqslant y \wedge y \leqslant z \to x \leqslant z) \wedge \forall x \forall y (x \leqslant y \vee y \leqslant x) \wedge \wedge \forall x \forall y (x \leqslant y \wedge y \leqslant x \to x = y) \wedge \forall x \exists y (x \leqslant y \wedge x \neq y) \, ,$$

(2) $$\mathfrak{A} \models \forall y_1 \ldots y_k \big(\exists y \varphi(y, y_1, \ldots, y_k) \to \exists y_0 \varphi(y_0, y_1, \ldots, y_k) \wedge \wedge \forall y^* (\varphi(y^*, y_1, \ldots, y_k) \to y_0 \leqslant y^*)\big) \, ,$$

für jedes $\varphi(y, y_1, \ldots, y_k) \in Y$.