102. Cyclic and Homogenous m-Semigroups

By F. M. SIOSON
University of Hawaii

(Comm. by Kinjirô KUNUGI, M.J.A., Sept. 12, 1963)

In a previous note [6], the author has indicated how a number of results in semigroups can be extended to more general algebraic systems consisting of an arbitrary associative m-ary operation. These latter systems may be called *m-semigroups*. Ordinary semigroups are thus 2-semigroups. A corresponding theory of *m-groups* has been in existence for quite some time (see W. Dörnte [1] and E. L. Post [4]).

In the present communication, we shall pursue further this trend of generalization in the particular topic mentioned in the title. The reader is referred to the previous paper [6] for other pertinent notions and definitions.

For any m-semigroup A, the subsystem $[a]$ generated by an element $a\in A$ consists of all admissible powers of a:

$$a=a^{\langle 0\rangle},\ a^m=a^{\langle 1\rangle},\cdots,\ a^{k(m-1)+1}=a^{\langle k\rangle},\cdots.$$

Two instances are possible:

I. No pair of admissible powers of a are equal so that $[a]$ is countably infinite;

II. There exists two non-negative integers r and s with $r<s$ such that $a^{\langle r\rangle}=a^{\langle s\rangle}$. Without loss of generality s may be assumed to be the least possible such integer. Let $p=s-r$ so that $a^{\langle r\rangle}=a^{\langle r+p\rangle}$. Then by induction $a^{\langle r\rangle}=a^{\langle r+kp\rangle}$ for all integers $k\geqq 0$. On the other hand, for any non-negative integer n, one has $n=kp+i$, where $k\geqq 0$ and $0\leqq i<p$. Hence

$$a^{\langle r+n\rangle}=a^{\langle r+(kp+i)\rangle}=a^{\langle r+i\rangle}.$$

This means that every admissible power of a beyond the $\langle s-1\rangle$th is an element of the set

$$G_a=\{a^{\langle r\rangle},\ a^{\langle r+1\rangle},\cdots,\ a^{\langle s-1\rangle}\}.$$

Note that $a^{\langle x\rangle}=a^{\langle y\rangle}$ if and only if $x\equiv y\ (\mathrm{mod}\ p(m-1))$. The order of $[a]$ is thus $s=r+p$, where p is the order of G_a (or the *period* of a) and r is the *index* of a. A is said to be *cyclic* if and only if $A=[a]$ for some $a\in A$.

Note further that G_a is closed under the same m-ary operation in A and is therefore an m-subsemigroup of A. That it is an ideal of $[a]$ is evident. G_a is in fact a minimal ideal, for, if $x\in G_a$ and x_i belongs to any ideal $I\subseteqq G_a$, then by a property of m-groups there exist $m-1$ elements $x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_m\in G_a$ such that $(x_1\cdots x_{i-1}x_i x_{i+1}\cdots x_m)=x$. Thus $x\in I$ and therefore $G_a=I$. The maximality of

G_a as an m-subgroup is quite also obvious.

Now, to prove that G_a is indeed an m-group in the sense of E. L. Post [4]. Due to its obvious commutativity, it is sufficient to prove the unique solvability of the equation

$$(a^{\langle r+k_1\rangle}a^{\langle r+k_2\rangle}\cdots a^{\langle r+k_{m-1}\rangle}x)=a^{\langle r+k\rangle},$$

for any set of non-negative integers $0\leqq k, k_1,\cdots, k_{m-1}<p$. But $x=a^{\langle r+y\rangle}$ is a solution of the above equation if and only if

$$\sum_{i=1}^{m-1}\langle r+k_i\rangle+\langle r+y\rangle\equiv\langle r+k\rangle \pmod{p(m-1)}.$$

This means that

$$(m-1)\Big(\langle r\rangle+\sum_{i=1}^{m-1}k_i-k+y\Big)\equiv 0 \pmod{p(m-1)}$$

or

$$\langle r\rangle+\sum_{i=1}^{m-1}k_i-k+y\equiv 0 \pmod{p}.$$

Since this last congruence always has a unique solution in y, $0\leqq y<p$, it follows then that the above mentioned equation also always has a unique solution. Whence G_a is an m-group.

Now, to show that G_a is cyclic, it suffices to show that for each integer $n\geqq 0$,

$$(a^{\langle r+n\rangle})^{\langle p\rangle}=a^{\langle r+n\rangle},$$

and that there exists an integer N such that no lower non-$\langle 0\rangle$ admissible power of $a^{\langle r+N\rangle}$ than the $\langle p\rangle$th equals itself.

For each i, $(a^{\langle r+n\rangle})^{\langle i\rangle}=a^{\langle r+n\rangle}$ if and only if

$$\langle (r+n)i(m-1)+(r+n)+i\rangle\equiv\langle r+n\rangle \pmod{p(m-1)}.$$

Hence $$(m-1)((r+n)i(m-1)+i)\equiv 0 \pmod{p(m-1)}$$

and therefore, $((r+n)(m-1)+1)i\equiv 0 \pmod{p}$.

Hence, by taking $i=p$, the first result mentioned above is obtained. The existence of an N is assured since there exists an infinite number of primes of the form $k(m-1)+1$. If $(r+N)(m-1)+1$ denotes any one of these primes which is different from all the prime factors of p, then

$$((r+N)(m-1)+1)i\equiv 0 \pmod{p}$$

if and only if $i\equiv 0 \pmod{p}$. Whence,

$$G_a=\{a^{\langle r+N\rangle}, (a^{\langle r+N\rangle})^{\langle 1\rangle},\cdots, (a^{\langle r+N\rangle})^{\langle p-1\rangle}\}.$$

We summarize all these in the following

THEOREM 1. *Let A be any m-semigroup with $a\in A$. If the m-subsemigroup $[a]$ generated by a is infinite, then all admissible powers of a are distinct. If $[a]$ is finite, then there exists integers r (called the index of a) and p (called the period of a) such that $a^{\langle r\rangle}=a^{\langle r+p\rangle}$ and*

$$[a]=\{a^{\langle 0\rangle}, a^{\langle 1\rangle},\cdots, a^{\langle r+p-1\rangle}\},$$

where $r+p$ is the order of $[a]$. Furthermore,

$$G_a=\{a^{\langle r\rangle}, a^{\langle r+1\rangle},\cdots, a^{\langle r+p-1\rangle}\}$$

is a maximal cyclic m-subgroup and also a minimal ideal of $[a]$.

The following are obvious consequences:

COROLLARY 1.1. *There exists for each pair of non-negative integers r and s a cyclic m-semigroup of index r and period p.*

COROLLARY 1.2. *Two finite cyclic m-semigroups are isomorphic if and only if they have the same index and the same period.*

COROLLARY 1.3. *Any two infinite cyclic m-semigroups are isomorphic.*

An m-semigroup A is *i-cancellative* (for any fixed $i=1,\cdots,m$) if and only if $(x_1x_2\cdots x_i\cdots x_m)=(y_1y_2\cdots y_i\cdots y_m)$ and $x_j=y_j$ for all $j\neq i$ implies $x_i=y_i$. Similarly, an element e is said to be an *i-identity* if and only if $(e\cdots \overset{i}{x}\cdots e)=x$ for $x\in A$. An i-identity for all $i=1,\cdots,m$ is simply called an *identity*.

COROLLARY 1.4. *If an m-semigroup is i-cancellative for any fixed $i=1,\cdots,m$, then every element of finite order is of index* 0.

In direct contrast with ordinary semigroups, a finite cyclic m-semigroup $[a]$ does not necessarily always possess an idempotent, i.e. an element e such that $e^{\langle 1\rangle}=e$. Consider, for example, the 3-semigroup $A=\{a, a^3, a^5, a^7, a^9, a^{11}, a^{13}\}$ generated by the element a such that $a^7=a^{15}$. Then $(aaa)=a^3$, $(a^3a^3a^3)=a^9$, $(a^5a^5a^5)=a^7$, $(a^7a^7a^7)=a^{13}$, $(a^9a^9a^9)=a^{11}$, $(a^{11}a^{11}a^{11})=a^9$, and $(a^{13}a^{13}a^{13})=a^7$.

The pertinent result in this regard is the following

THEOREM 2. *For each element a with finite index r and period p in an m-semigroup A, $[a]$ possesses a unique idempotent if and only if*

$$(m-1)x+\langle r\rangle\equiv 0 \pmod p$$

has a solution in non-negative integers. If it exists, the idempotent of $[a]$ is also the identity element of G_a.

Proof. The element $a^{\langle r+x\rangle}$ is an idempotent if and only if

$$m\langle r+x\rangle\equiv\langle r+x\rangle \pmod{p(m-1)}$$

or

$$(m-1)\langle r+x\rangle\equiv 0 \pmod{p(m-1)},$$

and hence, if and only if,

$$(m-1)x+\langle r\rangle\equiv 0 \pmod p.$$

From number theory, recall that a linear congruence such as this possesses a solution if and only if $(m-1, p)$, the greatest common divisor of $m-1$ and p, divides $\langle r\rangle=r(m-1)+1$. Clearly, this is only possible when $(m-1,p)=1$ and therefore there can also be only one idempotent in $[a]$.

Now, to show that an element $a^{\langle r+x\rangle}$ such that $(m-1)x+\langle r\rangle\equiv 0$ $(\mathrm{mod}\, p)$, that is to say an idempotent of $[a]$, is an identity of G_a, consider an arbitrary element $a^{\langle r+y\rangle}$ of G_a. Since

$$\begin{aligned}(mr+(m-1)x+y+1)(m-1)+1&=([(r+x)(m-1)+1]+(r+y))(m-1)+1\\&\equiv(r+y)(m-1)+1 \pmod p,\end{aligned}$$

then $(a^{\langle r+x\rangle}a^{\langle r+x\rangle}\cdots a^{\langle r+x\rangle}a^{\langle r+y\rangle}a^{\langle r+x\rangle}\cdots a^{\langle r+x\rangle})=a^{\langle mr+(m-1)x+y+1\rangle}=a^{\langle r+y\rangle}$ for all non-negative integers y.

COROLLARY 2.1. *In an ordinary semigroup (i.e. a 2-semigroup), the subsemigroup generated by an element, if it is of finite order, possesses a unique idempotent.*

This is clear, since $m-1=1$ in this case.

COROLLARY 2.2 (Post [4]). *A cyclic m-group G possesses a unique idempotent if and only if its order is prime to $m-1$.*

An m-semigroup A is *periodic* if and only if every element of A is of finite order, e.g. a finite m-semigroup. It is called *homogenous* if and only if for each element $a \in A$, $[a]$ contains an idempotent. Still another definition: an m-ary algebraic system is *entropic* if and only if

$$\begin{aligned}((a_{11}a_{12}\cdots a_{1m})(a_{21}a_{22}\cdots a_{2m})\cdots(a_{m1}a_{m2}\cdots a_{mm}))\\ =((a_{11}a_{21}\cdots a_{m1})(a_{12}a_{22}\cdots a_{m2})\cdots(a_{1m}a_{2m}\cdots a_{mm}))\end{aligned}$$

for any m by m matrix (a_{ij}) of elements from A. Obviously, commutativity implies entropy and, under the presence of an identity element, entropy implies both commutativity and associativity (see [2]).

It will be convenient, before going any further, to note the following obvious lemmata:

LEMMA A. *The collection of all non-negative integers form a commutative semigroup under the operation $*$ defined by*

$$a^{\langle s_1\rangle * \langle s_2\rangle}=(a^{\langle s_1\rangle})^{\langle s_2\rangle}$$

or $$\langle s_1\rangle * \langle s_2\rangle=\langle s_1 s_2(m-1)+s_1+s_2\rangle.$$

Its verification is direct. In fact, it is easy to see that $\langle s_1\rangle * \langle s_2\rangle * \cdots * \langle s_n\rangle=\sum_{i=1}^{n}\sigma_i(s_1, s_2,\cdots, s_n)(m-1)^{i-1}$, where σ_i denotes the ith elementary symmetric function of the s's.

LEMMA B. *For each integer $n \geqq 0$ and any set of elements $x_1, \cdots, x_m$ belonging to an entropic m-ary system,*

$$(x_1x_2\cdots x_m)^{\langle n\rangle}=(x_1^{\langle n\rangle}x_2^{\langle n\rangle}\cdots x_m^{\langle n\rangle}).$$

The proof is by induction.

The following result generalizes a theorem of S. Schwarz [5] on 2-semigroups.

THEOREM 3. *An entropic and homogenous m-semigroup A is the disjoint union of m-subsemigroups S_e (called maximal unipotent m-subsemigroups of A) each containing only one idempotent $e \in A$ such that $(S_{e_1}S_{e_2}\cdots S_{e_m}) \subseteqq S_{(e_1e_2\cdots e_m)}$ for any set $e_1, e_2,\cdots, e_m$ of idempotents in A.*

Proof: Let E be the set of all idempotents in A. Since A is entropic, E is clearly an m-subsemigroup of A.

For each $e \in E$, let $S_e=\{x: x^{\langle n\rangle}=e$ for some integer $n \geqq 0\}$. If $e \neq e'$

where e, $e' \in E$, then $S_e \frown S_{e'} = \phi$. For, if not, then $x^{\langle r\rangle} = e$ and $x^{\langle s\rangle} = e$ for some $x \in A$. But then $e = e^{\langle s\rangle} = (x^{\langle r\rangle})^{\langle s\rangle} = x^{\langle r\rangle * \langle s\rangle} = x^{\langle s\rangle * \langle r\rangle} = (x^{\langle s\rangle})^{\langle r\rangle} = e'^{\langle r\rangle} = e'$, which is a contradiction!

S_e, for each $e \in E$, is also an m-semigroup under the same operation in A. For, if $x_1, x_2, \cdots, x_m \in S_e$ so that

$$x_1^{\langle n_1\rangle} = x_2^{\langle n_2\rangle} = \cdots = x^{\langle n_m\rangle} = e$$

for some non-negative integers $n_1, n_2, \cdots, n_m$, then

$$(x_1 x_2 \cdots x_m)^{\langle n_1\rangle * \langle n_2\rangle * \cdots * \langle n_m\rangle} = ((x_1^{\langle n_1\rangle})^{\langle n_2\rangle * \cdots * \langle n_m\rangle} (x_2^{\langle n_2\rangle})^{\langle n_1\rangle * \cdots * \langle n_m\rangle} \cdots (x_m^{\langle n_m\rangle})^{\langle n_1\rangle * \cdots * \langle n_{m-1}\rangle}) = (ee \cdots e) = e.$$

By homogeneity of A, it then follows that $A = \bigcup_{e \in E} S_e$.

Finally, let $x_1 \in S_{e_1}, x_2 \in S_{e_2}, \cdots, x_m \in S_{e_m}$ where $e_1, \cdots, e_m \in E$ so that

$$x_1^{\langle n_1\rangle} = e_1,\ x_2^{\langle n_2\rangle} = e_2, \cdots, x_m^{\langle n_m\rangle} = e_m$$

for some non-negative integers $n_1, n_2, \cdots, n_m$. Then $(x_1 x_2 \cdots x_m)^{\langle n_1\rangle * \langle n_2\rangle * \cdots * \langle n_m\rangle} = ((x_1^{\langle n_1\rangle})^{\langle n_2\rangle * \cdots * \langle n_m\rangle} (x_2^{\langle n_2\rangle})^{\langle n_1\rangle * \cdots * \langle n_m\rangle} \cdots (x_m^{\langle n_m\rangle})^{\langle n_1\rangle * \cdots * \langle n_{m-1}\rangle}) = (e_1 e_2 \cdots e_m)$. Hence the result $(S_{e_1} S_{e_2} \cdots S_{e_n}) \subseteqq S_{(e_1 e_2 \cdots e_n)}$.

In [3], K. Iséki generalized the same result of S. Schwarz mentioned above in another direction, utilizing the notion of *strong reversibility* introduced by O. Thierrin [7]. Iseki's generalization may still be generalized as follows.

An m-semigroup A will be called *strongly reversible* if and only if for each $x_1, x_2, \cdots, x_m \in A$, there exists non-negative integers $n, n_1, \cdots, n_m$ such that

$$(x_1 x_2, \cdots, x_m)^{\langle n\rangle} = (x_{\phi(1)}^{\langle n_{\phi(1)}\rangle} x_{\phi(2)}^{\langle n_{\phi(2)}\rangle} \cdots x_{\phi(1)}^{\langle n_{\phi(m)}\rangle})$$

for any permutation ϕ of $1, 2, \cdots, m$. Note that any commutative m-semigroup is strongly reversible.

THEOREM 4. *A strongly reversible and homogenous m-semigroup A is the disjoint union of maximal unipotent m-subsemigroups S_e each containing only one idempotent e and such that*

$$(S_{e_1} S_{e_2} \cdots S_{e_m}) \subseteqq S_{(e_1 e_2 \cdots e_m)},$$

for any set of idempotents $e_1, e_2, \cdots, e_m$ in A.

Proof: Clearly, strong reversibility also implies that the idempotents of A form an m-subsemigroup E.

Let S_e be defined as in Theorem 3 and $x_1, x_2, \cdots, x_m \in S_e$ so that

$$x_1^{\langle s_1\rangle} = x_2^{\langle s_2\rangle} = \cdots = x_m^{\langle s_m\rangle} = e$$

for some non-negative integers $s_1, s_2, \cdots, s_m$. Strong reversibility then asserts that there exists non-negative integers $n, n_1, \cdots, n_m$ such that

$$(x_1 x_2 \cdots x_m)^{\langle n\rangle} = (x_{\phi(1)}^{\langle n_{\phi(1)}\rangle} x_{\phi(2)}^{\langle n_{\phi(2)}\rangle} \cdots x_{\phi(m)}^{\langle n_{\phi(m)}\rangle})$$

for any permutation ϕ of $1, 2, \cdots, m$. Remembering then that the elements on the right of the previous equality commute, we obtain

$$(x_1 x_2 \cdots x_m)^{\langle n\rangle * \langle s_1\rangle * \cdots * \langle s_m\rangle} = (x_{\phi(1)}^{\langle n_{\phi(1)}\rangle} x_{\phi(2)}^{\langle n_{\phi(2)}\rangle} \cdots x_{\phi(m)}^{\langle n_{\phi(m)}\rangle})^{\langle s_1\rangle * \cdots * \langle s_m\rangle}$$
$$= (x_1^{\langle n_1\rangle * \langle s_1\rangle * \cdots * \langle s_m\rangle} x_2^{\langle n_2\rangle * \langle s_1\rangle * \cdots * \langle s_m\rangle} \cdots x_m^{\langle n_m\rangle * \langle s_1\rangle * \cdots * \langle s_m\rangle}) = (ee \cdots e) = e.$$

The proof of the remainder of the theorem is the same as in

Theorem 3 except that here the commutativity of certain powers of elements from A is utilized.

References

[1] W. Dörnte: Untersuchungen über einen verallgemeinerten Gruppenbegriff, Mathematische Zeitschrift, **29**, 1–19 (1928).

[2] T. Evans: Abstract mean values, Duke Mathematical Journal, **30**, 331–347 (1963).

[3] K. Iséki: Contribution to the theory of semigroups. I, Proceedings of the Japan Academy, **32**, 174–175 (1956).

[4] E. L. Post: Polyadic groups, Transactions of the American Mathematical Society, **48**, 208–350 (1940).

[5] S. Schwarz: K teorii periodicheckih polugrupp (Contribution to the theory of periodic semigroups), Czechoslovak Mathematical Journal, **3**, 7–21 (1953).

[6] F. M. Sioson: On regular algebraic systems, Proceedings of the Japan Academy, **39**, 283–286 (1963).

[7] G. Thierrin: Sur quelques propriétés de certaines classes de demigroupes, Comptes Rendus, Paris, **239**, 1335–1337 (1954).