Pacific Journal of Mathematics

GENERATING MONOMIALS FOR FINITE SEMIGROUPS

DONALD C. RAMSEY

Vol. 39, No. 3 July 1971

PACIFIC JOURNAL OF MATHEMATICS
Vol. 39, No. 3, 1971

GENERATING MONOMIALS FOR FINITE SEMIGROUPS

DONALD C. RAMSEY

In this paper consideration is given semigroups which arise from a group $(G, \cdot)$ by defining a binary operation $\circ$ on G by the rule

$$x \circ y = x\phi y\psi \qquad \text{for all } x, y \text{ in } G,$$

where ϕ, ψ are endomorphisms of G. In particular, the structure of such semigroups is determined. Also determined are the structure and number of semigroups that can be defined by

$$x \circ y = ax^s y^t \qquad \text{for all } x, y \text{ in } G,$$

where $(G, \cdot)$ is a finite abelian group containing a, and s, t are nonnegative integers.

1. Introduction. Let $(G, \cdot)$ be a groupoid and let ϕ, ψ be transformations of G. A possibly different groupoid $(G, \circ)$ is defined by the rule

$$x \circ y = x\phi y\psi \qquad \text{for all } x, y \text{ in } G.$$

In § 2 of this paper we assume that $(G, \cdot)$ is a finite abelian group and define a groupoid $(G, \circ)$ by the rule

$$x \circ y = ax^s y^t \qquad \text{for all } x, y \text{ in } G,$$

where s, t are nonnegative integers and $a \in G$. Necessary and sufficient conditions on a, s, and t are found in order for $(G, \circ)$ to be a semigroup. Also, we determine the number of nonequivalent (i.e., non-isomorphic, non-anti-isomorphic) semigroups that are defined in this manner. Whenever the rule

$$x \circ y = ax^s y^t \qquad \text{for all } x, y \text{ in } G,$$

defines a semigroup, we say that $(G, \circ)$ *is generated by the monomial* ax^sy^t *over* $(G, \cdot)$.

In § 3 it is shown that if a semigroup $(G, \circ)$ is defined by the rule

$$x \circ y = x\phi y\psi \qquad \text{for all } x, y \text{ in } G,$$

where ϕ, ψ are endomorphisms of the group $(G, \cdot)$, then $(G, \circ)$ is an inflation of the direct product of a group and a rectangular band. Consequently, a semigroup generated by a monomial over a finite abelian group is an inflation of the direct product of a group and a rectangular band. Finally, if $(F_q, +, \cdot)$ is a finite field of order q and if the rule

$$x \circ y = ax^s y^t \qquad \text{for all } x,\ y \text{ in } F_q\ ,$$

where $a \in F_q$ defines a semigroup $(F_q, \circ)$, then $(F_q, \circ)$ is an inflation of the direct product of a cyclic group and a rectangular band, together with a zero element. This is a generalization of the results obtained in [3] by Plemmons and Yoshida.

2. Generating monomials. Throughout this section let $(G, \cdot)$ be a finite abelian group with identity element e, and let M denote the least common multiple of the orders of the elements of G. Then M is the least positive integer q such that $x^q = e$ for all x in G. The following theorem gives necessary and sufficient conditions on a monomial $ax^s y^t$ over $(G, \cdot)$, in order for it to generate a semigroup.

THEOREM 1. *The monomial* $ax^s y^t$ *generates a semigroup over* $(G, \cdot)$ *if and only if*
(i) $a^{s-t} = e$ *and*
(ii) $s^2 - s$ *and* $t^2 - t$ *are multiples of* M.

Proof. The monomial $ax^s y^t$ generates a semigroup over $(G, \cdot)$ if and only if for all x, y, z in G

$$a(ax^s y^t)^s z^t = ax^s(ay^s z^t)^t$$

which holds if and only if for all x, y, z in G

$$a^{s+1} x^{s^2} y^{st} z^t = a^{t+1} x^s y^{st} z^{t^2}$$

which in turn holds if and only if for all x, z in G

$$a^{s-t} x^{s^2-s} = z^{t^2-t}\ . \tag{2.1}$$

Assuming that (i) and (ii) hold, it follows that (2.1) holds since each side of the equation reduces to e. Thus $ax^s y^t$ generates a semigroup. Conversely, if $ax^s y^t$ generates a semigroup then equation (2.1) holds for all x, z in G, and in particular when $x = z = e$, so that $a^{s-t} = e$. By letting $z = e$ in equation (2.1) and replacing a^{s-t} by e, we get that $x^{s^2-s} = e$ for all x in G, whence $s^2 - s$ is a multiple of M. In a similar fashion it can be shown that $t^2 - t$ is a multiple of M.

If $s \geqq M$, then $s = qM + r$ for some integers q and r, where $q > 0$ and $0 \leqq r < M$, so that

$$ax^s y^t = ax^r y^t \qquad \text{for all } x,\ y \text{ in } G\ .$$

Hence, in searching for the number of nonequivalent semigroups generated by monomials over $(G, \cdot)$ we can assume that $0 \leqq s < M$ and $0 \leqq t < M$. Also, since the semigroup generated by ax^ty^s is anti-isomorphic to the one generated by ax^sy^t we can assume that $t \leqq s$. Furthermore, the following lemma shows that we need only consider monomials with $a = e$.

LEMMA 1. *Suppose ax^sy^t generates a semigroup $(G, \circ)$ over $(G, \cdot)$. Let $(G, *)$ be the semigroup generated by x^sy^t and let k denote the order of a in $(G, \cdot)$. Let m be the solution to the congruence*

$$(2t - 1)x \equiv 1 \pmod{k}.$$

Then m is unique (mod k) *and the mapping α from G into G defined by*

$$x\alpha = a^m x \qquad \textit{for all } x \textit{ in } G\,,$$

is an isomorphism of $(G, \circ)$ onto $(G, *)$.

Proof. Since k is the order of a in $(G, \cdot)$, it follows that $k \mid M$. Since ax^sy^t generates a semigroup, $M \mid t^2 - t$, whence $k \mid t^2 - t$. Therefore, the greatest common divisor of $2t - 1$ and k must divide $(2t - 1)^2 - 4(t^2 - t) = 1$, whence $2t - 1$ and k are relatively prime. Hence [2, Theorem 3-11, p. 34] there exists a unique solution m (mod k) to the congruence

$$(2t - 1)x \equiv 1 \pmod{k}\,.$$

Therefore k is a factor of $m(2t - 1) - 1$. Now, the mapping α from G into G defined by

$$\alpha : z \longrightarrow a^m z$$

is a permutation of G. Let x, y be arbitrary elements of G. Then

$$\begin{aligned}(x\alpha) * (y\alpha) &= (a^m x)^s (a^m y)^t \\ &= a^{m(s+t)} x^s y^t \\ &= a^{m+1} x^s y^t\end{aligned}$$

since

$$a^{m(s+t)-(m+1)} = a^{m(s+t-1)-1} = a^{m(s-t)+m(2t-1)-1} = e\,.$$

Therefore,

$$\begin{aligned}(x\alpha) * (y\alpha) &= a^{m+1} x^s y^t \\ &= (ax^sy^t)\alpha \\ &= (x \circ y)\alpha\,.\end{aligned}$$

Thus α is an isomorphism of $(G, \circ)$ onto $(G, *)$.

Let n denote the order of $(G, \cdot)$ and let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the prime power factorization of n, where $p_i \neq p_j$ if $i \neq j$, and $\alpha_i > 0$ for $1 \leqq i \leqq r$. By the fundamental theorem for finite abelian groups, G has the structure $S(p_1) \times S(p_2) \times \cdots \times S(p_r)$ where each $S(p_i)$ is the Sylow p-subgroup of $(G, \cdot)$ of order $p_i^{\alpha_i}$ for $1 \leqq i \leqq r$. The order of any element in $S(p_i)$ is a power of the prime p_i so that for each prime p_i with $1 \leqq i \leqq r$, there exists an element $x_i \in G$ having order a power > 0 of p_i. Thus the prime power factorization of M is $M = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$ where $0 < \gamma_i \leqq \alpha_i$ for $1 \leqq i \leqq r$.

For each integer m let

$$G_m = \{x \in G: x^m = e\} .$$

Let s be a positive integer such that $M \mid s(s-1)$. Since s and $s-1$ are relatively prime, the prime factors of M which divide s do not divide $s-1$, and those dividing $s-1$ do not divide s. Assume that the indexing of the primes p_i in the factorization of M is such that $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_j^{\gamma_j} \mid (s-1)$ and $p_{j+1}^{\gamma_{j+1}} p_{j+2}^{\gamma_{j+2}} \cdots p_r^{\gamma_r} \mid s$. Identifying the elements of G and $S(p_1) \times S(p_2) \times \cdots \times S(p_r)$ we get the following lemma.

LEMMA 2. *The set G_{s-1} is the subgroup $S(p_1) \times S(p_2) \times \cdots S(p_j)$ of G having order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j}$.*

Proof. Let $x \in G_{s-1}$. Written as an r-tuple, $x = (x_1, x_2, \cdots, x_r)$, so $x^{s-1} = (x_1^{s-1}, x_2^{s-1}, \cdots, x_r^{s-1}) = e_r$, where e_r is the r-tuple $(e, e, \cdots, e)$. In particular, $x_{j+1}^{s-1} = x_{j+2}^{s-1} = \cdots = x_r^{s-1} = e$. Since the orders of $x_{j+1}, x_{j+2}, \cdots, x_r$ are relatively prime to $s-1$ it follows that $x_{j+1} = x_{j+2} = \cdots = x_r = e$. Hence $x \in S(p_1) \times S(p_2) \times \cdots \times S(p_j)$. Conversely, let $x \in S(p_1) \times S(p_2) \times \cdots \times S(p_j)$. We write

$$x = (x_1, x_2, \cdots, x_j) .$$

Letting e_j denote the j-tuple $(e, e, \cdots, e)$, we have

$$e_j = x^{s(s-1)} = (x_1^{s(s-1)}, x_2^{s(s-1)}, \cdots, x_j^{s(s-1)}) ,$$

so that $x_1^{s(s-1)} = x_2^{s(s-1)} = \cdots = x_j^{s(s-1)} = e$. Since the orders of $x_1, x_2, \cdots, x_j$ are relatively prime to s, $x_1^{s-1} = x_2^{s-1} = \cdots = x_j^{s-1} = e$, whence $x^{s-1} = e_j$ and $x \in G_{s-1}$.

LEMMA 3. *Let s and s' be positive integers less than M such that $M \mid s^2 - s$ and $M \mid s'^2 - s'$. If the order of G_{s-1} is the same as the order of $G_{s'-1}$ then $s = s'$.*

Proof. By Lemma 2 the subgroups G_{s-1} and $G_{s'-1}$ are direct products of Sylow p-subgroups of G. Since the order of G_{s-1} is the same as the order of $G_{s'-1}$, it follows that the prime powers in the factorization of M which divide $s-1$ are exactly those which divide $s'-1$. Thus $M \mid s(s'-1)$ and $M \mid s'(s-1)$, whence

$$M \mid [s(s'-1) - s'(s-1)] ,$$

so $M \mid s'-s$. Since $-M < s' - s < M$, $s' - s = 0$, whence $s' = s$.

THEOREM 2. *Suppose $x^s y^t$ and $x^{s'} y^{t'}$ generate semigroups over $(G, \cdot)$, where $0 \leqq t \leqq s < M$ and $0 \leqq t' \leqq s' < M$. Then these semigroups are isomorphic if and only if $s = s'$ and $t = t'$.*

Proof. Clearly if $s = s'$ and $t = t'$ then $x^s y^t$ and $x^{s'} y^{t'}$ generate the same semigroup over $(G, \cdot)$. Conversely, suppose that $x^s y^t$ and $x^{s'} y^{t'}$ generate semigroups $(G, \circ)$ and $(G, *)$, respectively, and suppose $(G, \circ)$ is isomorphic to $(G, *)$. Then the Cayley tables for $(G, \circ)$ and $(G, *)$ must have the same number of distinct rows. That is, $(G, \circ)$ and $(G, *)$ must have the same number of distinct inner left translations [1, p. 9]. The distinct inner left translations of $(G, \circ)$ are determined by the distinct elements of the set $\{x^s \colon x \in G\}$. But

$$\{x^s \colon x \in G\} = G_{s-1}$$

as defined above. Thus the orders of G_{s-1} and $G_{s'-1}$ are equal, whence by Lemma 3, $s = s'$ if both s and s' are positive. If $s = 0$ then $G_{s'-1} = G_{s-1} = \{e\}$, so that $M \mid s'$, whence $s' = 0$. Similarly, if $s' = 0$ then $s = 0$, so that in any case $s = s'$. Dually, by considering columns in the Cayley tables of $(G, \circ)$ and $(G, *)$, we see that $t = t'$.

We now approach the problem of determining the number of nonequivalent semigroups of order n generated by monomials over $(G, \cdot)$. The integers s with $0 \leqq s < M$ that will serve as exponents in generating monomials are exactly those such that $M \mid s^2 - s$. Hence the set H of such integers is the solution set of the congruence

$$x^2 - x \equiv 0 \pmod{M} . \tag{2.2}$$

LEMMA 4. *The cardinality of the solution set H to the congruence (2.2) is 2^r, where r is the number of distinct primes in the prime power factorization of M.*

Proof. Let $M = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$ be the prime power factorization of M. Then x_0 is a solution to (2.2) if and only if x_0 is a simultaneous solution to the system of congruences

$$x^2 - x \equiv 0 \quad (\text{mod } p_i^{\gamma_i}) \quad 1 \leqq i \leqq r\,. \tag{2.3}$$

For each i, $1 \leqq i \leqq r$, suppose c_i is a solution to $x^2 - x \equiv 0 \ (\text{mod } p_i^{\gamma_i})$. Then, by the Chinese Remainder Theorem, there is a solution x_0 to the system

$$x \equiv c_1 \ (\text{mod } p_1^{\gamma_1}),\ x \equiv c_2 \ (\text{mod } p_2^{\gamma_2}),\ \cdots,\ x \equiv c_r \ (\text{mod } p_r^{\gamma_r})$$

which is unique modulo M. Then each r-tuple $(c_1, \cdots, c_r)$ gives rise to a unique solution (mod M) to system (2.3). Thus the number of solutions to (2.2) is the product of the numbers of roots of the congruences in (2.3). But, by § 3.5 of [2], the solution set to each of these congruences is $\{0, 1\}$, whence the cardinality of the solution set of (2.2) is 2^r.

Finally, we have the following theorem.

THEOREM 3. *The number N_G of nonequivalent semigroups generated by monomials over $(G, \cdot)$ is $2^{r-1}(2^r + 1)$, where r is the number of distinct primes which divide M.*

Proof. The pairs s, t of elements of H yield monomials $x^s y^t$ which generate semigroups over $(G, \cdot)$. Moreover, these are the only pairs modulo M which will do so. Thus to determine N_G we need only count the ways in which s and t can be picked from H with $t \leqq s$. There are

$$1 + 2 + 3 + \cdots + 2^r = \frac{2^r(2^r+1)}{2} = 2^{r-1}(2^r+1)$$

ways to do this.

3. Structure theorems. The following definition and facts are the contents of [1, p. 98, Exercise 10]. Let T be a semigroup. With each element α of T, associate a set X_α containing α such that the sets X_α are mutually disjoint. Let $s = \bigcup_{\alpha \in T} X_\alpha$, and let the product in T be extended to a product in S by defining $ab = \alpha\beta$ if $a \in X_\alpha$ and $b \in X_\beta$. Then S is a semigroup and is said to be an *inflation* of T. Now, T is a subsemigroup of S such that $S^2 \subseteqq T$. If we define a mapping θ from S into T by $a\theta = \alpha$ when $a \in X_\alpha$, then

(i) θ maps S *upon* T,

(ii) $\theta^2 = \theta$, and

(iii) $(a\theta)(b\theta) = ab$ for all $a, b \in S$.

Let T be a subsemigroup of S such that $S^2 \subseteqq T$, and let θ be a transformation of S having properties (i), (ii), and (iii) above. Then S is an inflation of T.

By a *left zero semigroup* we mean a semigroup S such that $xy = x$

for all $x, y \in S$. A *right zero semigroup* is defined dually.

THEOREM 4. *Let $(S, \cdot)$ be a semigroup such that for some transformation ϕ of S, $xy = x\phi$ for all $x, y \in S$. Then S is an inflation of the range $S\phi$ of ϕ, and $S\phi$ is a left zero semigroup. Conversely, each inflation of a left zero semigroup is obtained in this manner.*

Proof. Since S is a semigroup, $(xy)z = x(yz)$ for all $x, y, z \in S$, so $x\phi^2 = x\phi$ for all $x \in S$, whence $\phi^2 = \phi$ on S. Since $S^2 = S\phi$, $S\phi$ is a subsemigroup of S such that $S^2 \subseteqq S\phi$. Now ϕ maps S onto $S\phi$ and

$$a\phi b\phi = a\phi^2 = a\phi = ab \qquad \text{for all } a, b \in S .$$

Hence, S is an inflation of $S\phi$. Let $a, b \in S\phi$. Then $a = a\phi$, so

$$ab = a\phi b = a\phi^2 = a\phi = a ,$$

thus $S\phi$ is a left zero semigroup. Conversely, let $(S, \cdot)$ be an inflation of a left zero semigroup L. Since S is an inflation of L, S is the disjoint union of subsets X_a, where $a \in L \cap X_a$. Define a transformation ϕ of S by $x\phi = a$ if and only if $x \in X_a$. Let $x, y \in S$ with $x \in X_a$ and $y \in X_b$. Then $xy = ab = a = x\phi$.

COROLLARY 1. *If $(G, \circ)$ is generated by x^s over a finite abelian group $(G, \cdot)$, then $(G, \circ)$ is an inflation of the left zero semigroup $(L, \circ)$, where $L = \{x^s: x \in G\}$.*

By the dual of Theorem 4 we get the following corollary.

COROLLARY 2. *If $(G, \circ)$ is generated by y^t over the finite abelian group $(G, \cdot)$, then $(G, \circ)$ is an inflation of the right zero semigroup $(R, \circ)$, where $R = \{y^t: y \in G\}$.*

Before investigating the structure of semigroups generated by the more general monomial $x^s y^t$ with $0 \leqq t \leqq s < M$, we prove the following lemma.

LEMMA 5. *Suppose the semigroup $(G, \circ)$ is generated by $x^s y^t$ over an abelian group $(G, \cdot)$ with $0 \leqq t \leqq s < M$. Then $\circ$ is commutative if and only if $s = t$.*

Proof. Suppose $s = t$. Then for $x, y \in G$ we have

$$x \circ y = x^s y^s = y^s x^s = y \circ x .$$

Conversely, if $\circ$ is commutative, then $x \circ y = y \circ x$ for all $x, y \in G$, so that $x^s y^t = y^s x^t$ for all $x, y \in G$. Letting $y = e$, we see that $x^s = x^t$ for all $x \in G$, so that $M \mid s - t$. Thus $s - t = 0$, whence $s = t$.

Given an arbitrary group $(G, \cdot)$ and a pair of transformations ϕ, ψ of G, a groupoid $(G, \circ)$ is defined by the rule

$$x \circ y = x\phi y\psi \qquad \text{for all } x, y \text{ in } G .$$

We say that $(G, \circ)$ *is generated by the pair of transformations* (ϕ, ψ) *over* $(G, \cdot)$. If we insist that the transformations ϕ and ψ be endomorphisms, the following lemma gives necessary and sufficient conditions in order for $(G, \circ)$ to be a semigroup.

LEMMA 6. *Let $(G, \cdot)$ be an arbitrary group with identity element e, and let ϕ, ψ be endomorphisms of $(G, \cdot)$. Define a groupoid $(G, \circ)$ by the rule*

$$x \circ y = x\phi y\psi \qquad \textit{for all } x, y \textit{ in } G .$$

Then $(G, \circ)$ is a semigroup if and only if ϕ and ψ are idempotent and commute.

Proof. Assume that the groupoid $(G, \circ)$ is a semigroup. Then

$$(x \circ y) \circ z = x \circ (y \circ z) \qquad \text{for all } x, y, z \text{ in } G ,$$

so

$$(x\phi y\psi)\phi \cdot z\psi = x\phi(y\phi z\psi)\psi \qquad \text{for all } x, y, z \text{ in } G . \tag{3.1}$$

Upon setting $y = z = e$ in (3.1), we get

$$(x\phi)\phi = x\phi \qquad \text{for all } x \text{ in } G ,$$

since $e\phi = e\psi = e$. In a similar fashion $\psi^2 = \psi$. Letting $x = z = e$ in (3.1), we see that

$$(y\psi)\phi = (y\phi)\psi \qquad \text{for all } y \text{ in } G ,$$

hence $\phi\psi = \psi\phi$. Conversely, assume that $\phi^2 = \phi$, $\psi^2 = \psi$, and $\phi\psi = \psi\phi$. Then for arbitrary $x, y, z \in G$

$$\begin{aligned}(x \circ y) \circ z &= (x\phi y\psi)\phi \cdot z\psi \\ &= x\phi^2 \cdot y\psi\phi \cdot z\psi \\ &= x\phi \cdot y\phi\psi \cdot z\psi^2 \\ &= x\phi(y\phi z\psi)\psi \\ &= x \circ (y \circ z) .\end{aligned}$$

Thus $(G, \circ)$ is a semigroup.

The following definitions come from [1, p. 98, p. 25]. A semigroup S is called *stationary on the right* if for all a, b, c in S, $ab = ac$ implies $xb = xc$ for all $x \in S$. A semigroup S is called *E-inversive* if for each $a \in S$ there exists $x \in S$ such that ax is idempotent. Let a, b, x, y be elements of a semigroup S. Consider the four elements ax, ay, bx, by of S. We call S *rectangular* if, whenever three elements are equal, all four are equal. Let X and Y be any two sets, and define a binary operation in $S = X \times Y$ by

$$(x_1, y_1)(x_2, y_2) = (x_1, y_2)$$

where $x_1, x_2 \in X$ and $y_1, y_2 \in Y$. Then S is a semigroup called the *rectangular band* on $X \times Y$.

THEOREM 5. *Let $(G, \circ)$ be a semigroup generated by a pair of endomorphisms (ϕ, ψ) over the group $(G, \cdot)$. Then $(G, \circ)$ is an inflation of its kernel $G \circ G$ and its kernel is isomorphic to the direct product of a group and a rectangular band.*

Proof. By Lemma 6, $\phi^2 = \phi$, $\psi^2 = \psi$, and $\phi\psi = \psi\phi$. Now $(G, \circ)$ is stationary on the right, since if $a \circ b = a \circ c$ for arbitrary $a, b, c \in G$ then $a\phi b\psi = a\phi c\psi$, so $b\psi = c\psi$. Thus $x\phi b\psi = x\phi c\psi$ for all $x \in G$, so that $x \circ b = x \circ c$ for all $x \in G$. Let $a \in G$ and denote by a^{-1} its group inverse. Then

$$a \circ a^{-1} = a\phi(a\psi)^{-1} .$$

Now,

$$\begin{aligned}(a \circ a^{-1}) \circ (a \circ a^{-1}) &= (a\phi(a\psi)^{-1})\phi \cdot (a\phi(a\psi)^{-1})\psi \\ &= a\phi^2 \cdot (a\psi\phi)^{-1} \cdot a\phi\psi \cdot (a\psi^2)^{-1} \\ &= a\phi(a\psi)^{-1} \\ &= a \circ a^{-1}\end{aligned}$$

so $(G, \circ)$ *is* E-inversive since a was taken to be arbitrary in G. Let e denote the identity element of $(G, \cdot)$. Since $(G, \circ)$ is stationary on the right it is rectangular, whence by Theorem 8 of [4], $G \circ G$ is the kernel of G and

$$G \circ G \cong H \times E$$

where E is the rectangular band consisting of the idempotents of $(G, \circ)$, and H is the subgroup

$$e \circ G \circ e = \{x\phi\psi \colon x \in G\}$$

of $(G, \circ)$. By [5] the mapping $\theta\colon G \to G \circ G$ defined by $a\theta = a \circ f$, where

f is the identity element of the maximal subgroup to which $a \circ a$ belongs, is onto, idempotent, and $a\theta \circ b\theta = a \circ b$ for all $a, b \in G$, whence $(G, \circ)$ is an inflation of $(G \circ G, \circ)$. Thus $(G, \circ)$ is an inflation of the direct product of a group and a rectangular band. (We note that $(H, \cdot) = (H, \circ)$.)

The structure of a semigroup $(G, \circ)$ generated by the monomial $x^s y^t$ is revealed by the following theorem, which is a consequence of Theorem 5.

THEOREM 6. *Let $(G, \circ)$ be a semigroup generated by the monomial $x^s y^t$ over the finite abelian group $(G, \cdot)$. Then $(G, \circ)$ is an inflation of its kernel $G \circ G$, and its kernel is isomorphic to the direct product of the subgroup*

$$H = \{x^{st} : x \in G\}$$

of $(G, \circ)$ and the rectangular band

$$E = \{x \in G : x = x^{s+t}\} .$$

Proof. Let ϕ, ψ be defined on $(G, \cdot)$ by $x\phi = x^s$ and $y\psi = y^t$. Then ϕ, ψ are endomorphisms of $(G, \cdot)$ since $(G, \cdot)$ is abelian. Also, $\phi^2 = \phi$ and $\psi^2 = \psi$ since $x^{s^2} = x^s$ and $x^{t^2} = x^t$ for all $x \in G$. Since

$$(x^s)^t = x^{st} = (x^t)^s \qquad \text{for all } x \in G ,$$

it follows that ϕ and ψ commute. Thus ϕ and ψ as defined above satisfy the hypothesis of Theorem 5, so $(G, \circ)$ is an inflation of its kernel $(G \circ G, \circ)$. Since $x\phi\psi = x^{st}$ for $x \in G$, and since x is an idempotent of $(G, \circ)$ if and only if $x^{s+t} = x$, it follows that

$$G \circ G \cong H \times E$$

where H and E are as defined in the statement of the theorem.

Let (a, b) denote the greatest common divisor of integers a and b. We have the following lemma concerning certain subgroups of a cyclic group.

LEMMA 7. *Let G be a cyclic group of order n with identity element e, and let s be a nonnegative integer such that $n \mid s^2 - s$. Then $G_{s-1} = \{x \in G : x^{s-1} = e\}$ is a subgroup of G having order $(n, s-1)$.*

Proof. It follows immediately that G_{s-1} is a subgroup of G. Let m denote the order of G_{s-1}, and let $d = (n, s-1)$. Since

$$x^{s-1} = e = x^n , \qquad \text{for all } x \in G_{s-1} ,$$

it follows that $m \mid s-1$ and $m \mid n$, whence $m \leqq d$. Now, let a be a generator of G. Then $a^{n/d}$ generates a subgroup $[a^{n/d}]$ of G, of order d. But $(a^{n/d})^{s-1} = (a^n)^{(s-1)/d} = e$, so $a^{n/d} \in G_{s-1}$, whence $[a^{n/d}] \subseteqq G_{s-1}$. Thus $d \leqq m$, and so $m = d = (n, s-1)$.

The next theorem gives the structure of the group H in Theorem 6, whenever $(G, \cdot)$ is a cyclic group.

THEOREM 7. *If $(G, \circ)$ is a semigroup generated by the monomial $x^s y^t$ over the cyclic group $(G, \cdot)$ of order n, then $(G, \circ)$ is an inflation of its kernel $G \circ G$. Furthermore, its kernel is isomorphic to the direct product of the cyclic subgroup*

$$H = \{x^{st} : x \in G\}$$

of $(G, \circ)$ of order $(n, st-1)$ and the rectangular band

$$E = \{x \in G : x^{s+t} = x\} .$$

Proof. Suppose $x^s y^t$ generates a semigroup over $(G, \cdot)$. Then the set H defined above is the same as the set

$$G_{st-1} = \{x \in G : x^{st-1} = e\} .$$

Since $n \mid s^2 - s$, and $n \mid t^2 - t$, it follows that

$$n \mid (s^2 - s)t + s^2(t^2 - t) ,$$

whence $n \mid (st)^2 - st$. By Lemma 7, H has order $(n, st-1)$. The remaining part of the proof follows immediately from Theorem 6.

We conclude with a corollary to Theorem 7 which extends the results obtained in [3].

COROLLARY 3. *Let $(F_q, +, \cdot)$ be a finite field of order q, and let $(F_q, \circ)$ be a semigroup generated by $x^s y^t$ over $(F_q, \cdot)$. Then $(F_q, \circ)$ is an inflation of the direct product of a cyclic group of order $(q-1, st-1)$, and a rectangular band, together with a zero element.*

Proof. Let $F_q^* = F_q \backslash \{0\}$. Then $(F_q^*, \cdot)$ is the multiplicative group of $(F_q, +, \cdot)$, hence is a cyclic group of order $q-1$. By Theorem 7, $(F_q^*, \circ)$ is an inflation of the direct product of a cyclic group of order $(q-1, st-1)$, and a rectangular band. Since

$$F_q = F_q^* \cup \{0\}$$

and 0 is a zero for $\circ$, the corollary holds.

REFERENCES

1. A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, Vol. I, Mathematical Surveys 7, Amer. Math. Soc., Providence, R.I., 1961.
2. W. J. LeVeque, *Topics in Number Theory*, Vol. I, Addison-Wesley Publishing Co., Inc., Reading, Mass., 1956.
3. R. J. Plemmons and R. Yoshida, *Generating polynomials for finite semigroups*. To appear in Mathematishe Nachrichten.
4. G. Thierrin, *Demi-groups inverse's et rectangulaires*, Acad. Roy. Belg. Cl. Sci. (5) **41** (1955), 83-92, (MR 17, 10).
5. M. Yamada, *A note on middle unitary semigroups*, Kōdai Math. Semi. Rep., **7** (1955), 49-52, (MR 17, 585).

Received October 23, 1970. This research is a portion of the author's doctoral dissertation written at the University of Tennessee under the direction of Dr. R. J. Plemmons.

UNIVERSITY OF TENNESSEE

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. The editorial "we" must not be used in the synopsis, and items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. Index to Vol. **39**. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is $8.00; single issues, $3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues $1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 270, 3-chome Totsuka-cho, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics
Vol. 39, No. 3 July, 1971