# ON SEMISIMPLE COMMUTATIVE SEMIGROUPS

BY

B. D. ARENDT[1]

ABSTRACT. This paper presents an application of radical theory to the structure of commutative semigroups via their semilattice decomposition. Maximal group congruences and semisimplicity are characterized for certain classes of commutative semigroups and $N$-semigroups.

The concepts of a radical theory and semisimplicity in semigroups analogous to that of ring theory have been studied by a number of authors, both as a general theory, and applied to specific classes of semigroups. (See e.g. [1], [3], [5]–[9].) In this paper we apply these techniques to a study of the structure of commutative semigroups.

Every semigroup $S$ has a least congruence $\mu$ such that $S/\mu$ is a semilattice $Y$. Each congruence class of $\mu$ is a subsemigroup of $S$, and the collection $\{S_\alpha\}$, $\alpha \in Y$, of congruence classes is called the greatest *semilattice decomposition* of $S$. Conversely, if $Y$ is a semilattice and $\{S_\alpha\}$, $\alpha \in Y$, is a collection of pairwise disjoint semigroups, then any semigroup $S = \bigcup \{S_\alpha : \alpha \in Y\}$ with the property that $S_\alpha S_\beta \subseteq S_{\alpha\beta}$ for $\alpha, \beta \in Y$ is a *semilattice composition* of the $S_\alpha$. Thus a natural approach to the structure of a given type of semigroup is through a characterization of the semilattice decompositions, the structure of the $S_\alpha$, and the semilattice compositions. The semilattice decomposition of commutative semigroups was described by Tamura and Kimura [12]. In this case the semigroups $S_\alpha$ are the maximal archimedean subsemigroups, where $S_\alpha$ archimedean means given any two elements of $S_\alpha$ each divides some power of the other. Conversely, the general solution of the semilattice composition problem is known (see [10, Theorem III.7.2]).

If $\tau$ is a congruence on a semigroup $S$, we say $\tau$ is *modular* if there exists an element $e$ in $S$ such that $(ex)\tau(xe)\tau x$ for all $x$ in $S$. The *radical*

---

congruence $\rho$ is defined to be the intersection of all the maximal, modular congruences on $S$, and $S$ is said to be *semisimple* if $\rho = \iota$, the identity relation. We begin here a study of semisimple commutative semigroups. The semilattice decomposition of such semigroups is described, and we obtain partial results on the nature of the $S_\alpha$ and semilattice compositions. As a related problem, we also obtain conditions for the existence of maximal group congruences on certain classes of $N$-semigroups. My thanks to the referee for the suggestion of Theorem 3.

If $S$ is a commutative semigroup, a mapping $\phi$ from $S$ into $S$ is a *translation* if $(xy)\phi = x(y\phi)$ for all $x$, $y$ in $S$. We denote by $T(S)$ the set of all translations of $S$. If the commutative semigroup $S$ is a semilattice of subsemigroups $S_\alpha$ and $\alpha > \beta$, then $S_\alpha \cup S_\beta$ is evidently an ideal extension of $S_\beta$ by $S_\alpha \cup \{0\}$. For each $a \in S_\alpha$, let the mapping $\phi_a$ be defined on $S_\beta$ by $x\phi_a = xa$ for all $x \in S_\beta$. Then $\phi_a \in T(S_\beta)$ and $\phi_{\alpha\beta}: a \rightarrow \phi_a$ is a homomorphism from $S_\alpha$ into $T(S_\beta)$. Further, every such homomorphism determines an extension $S_\alpha \cup S_\beta$ with multiplication defined in the obvious way [13].

Oehmke [9] has characterized maximal modular congruences on a commutative semigroup, and we state his result as a lemma.

**Lemma 1.** *Let $S$ be a commutative semigroup and $r$ a maximal modular congruence on $S$. Then either*

(i) *$S/r$ is a cyclic group of prime order, or*

(ii) *$S/r$ is the semilattice $\{0, 1\}$.*

**Theorem 2.** *Let $S$ be a commutative semisimple semigroup and let $S = \bigcup S_\alpha$, $\alpha \in Y$, be the greatest semilattice decomposition of $S$. Then each $S_\alpha$ is semisimple and cancellative, and $\alpha > \beta$ implies $S_\alpha$ is isomorphically embedded in $T(S_\beta)$.*

**Proof.** Let $x$, $y \in S_\alpha$, then $S$ semisimple implies there exists a maximal, modular congruence $r$ on $S$ such that $x \not\equiv y \pmod{r}$. The restriction $r_\alpha$ of $r$ to $S_\alpha$ is clearly a congruence on $S_\alpha$. Further, if $r$ is of type (ii) (Lemma 1) then $r_\alpha$ cannot separate elements of $S_\alpha$ since $S_\alpha$ is archimedean and has no proper prime ideals. Thus $r$ and hence $r_\alpha$ must be of type (i). It follows that $r_\alpha$ is a maximal modular congruence on $S_\alpha$, so $S_\alpha$ is semisimple. The fact that all the maximal, modular congruences on $S_\alpha$ are cancellative and their intersection is the identity congruence says $S_\alpha$ must be cancellative. Suppose $\alpha > \beta$ and $a$, $b \in S_\alpha$ with $a\phi_{\alpha\beta} = b\phi_{\alpha\beta}$, that is, $ca = cb$ for $c \in S_\beta$. If $r$ is any maximal, modular congruence on $S$ of type (i) then obviously $(ca)r(cb)$ and thus $arb$ since $r$ is cancellative. If $r$ is a type (ii) congruence

then again $a \tau b$ holds since $a$ and $b$ are in the same archimedean component. It follows that $a \tau b$ for all maximal, modular congruences $\tau$ on $S$, and by semisimplicity, $a = b$. Thus $\phi_{\alpha\beta}$ is one-to-one, proving the theorem.

Each $S_\alpha$ of the theorem is thus a commutative, cancellative, archimedean semigroup. If $S_\alpha$ contains an idempotent then it is an abelian group. If such a semigroup does not contain an idempotent it is called an *N-semi-group*. To complete a characterization of commutative semisimple semigroups it is now necessary to describe the semisimple archimedean components $S_\alpha$, and then determine those semilattice compositions of the $S_\alpha$ which are semisimple. It is evident that an abelian group $G$ is semisimple if and only if the Frattini subgroup of $G$ is trivial, that is, $\bigcap \{G^p : p \text{ is a prime}\} = \{e\}$. If, in addition, $G$ is periodic (torsion), then $G$ is semisimple if and only if each of its $p$-primary components is elementary abelian. If $G$ is finitely generated, it is semisimple if and only if its torsion subgroup is semisimple.

**Theorem 3.** *Let $S$ be a semilattice of abelian groups $\{G_\alpha : \alpha \in Y\}$, with linking homomorphisms $\phi_{\alpha,\beta}$. Then the following are equivalent.*

(i) *$S$ is semisimple.*

(ii) *Each $\phi_{\alpha,\beta}$, $\alpha \geq \beta$, is one-to-one and the direct limit $\varinjlim G_\alpha$ is semisimple.*

(iii) *$S$ is the subdirect product of a semilattice and a semisimple group.*

**Proof.** We show (i) $\Longleftrightarrow$ (iii) $\Longleftrightarrow$ (ii). (i) $\Longleftrightarrow$ (iii) is obvious.

Suppose (iii). Then, by Theorem 2, each $\phi_{\alpha,\beta}$ is 1-1. Further the maximum group homomorphic image $S/\sigma$ is isomorphic to $\varinjlim G_\alpha$; here $\sigma = \{(a, b) \in S \times S : ea = eb \text{ for some } e^2 = e \in S\}$.

Suppose $S \subseteq E \times G$ where $G$ is semisimple. Then the projection $\pi$ of $S$ onto $G$ is a group homomorphism so that $\sigma \subseteq \pi \circ \pi^{-1}$. On the other hand, let $a = (a_1, a_2)$, $b = (b_1, b_2)$ be in $S$ and suppose $a\pi = b\pi$. Then $a_2 = b_2$ and so $aa^{-1}bb^{-1}a = aa^{-1}bb^{-1}b$; that is $\pi \circ \pi^{-1} \subseteq \sigma$. Hence $\sigma = \pi \circ \pi^{-1}$ and $G \cong S/\sigma \cong \varinjlim G_\alpha$. Thus (ii) holds.

Assume (ii). Since each $G_\alpha$ is a group, $T(G_\alpha)$ is isomorphic to $G_\alpha$, so for $\alpha > \beta$ we have $G_\alpha$ is embedded in $G_\beta$. Let $a$ and $b$ be distinct elements of $S$. If $a$ and $b$ are in different $G_\alpha$ then it is clear that there is a maximal modular congruence of type (ii) (Lemma 1) which separates $a$ and $b$, so assume $a$, $b \in G_\alpha$. If $e_\beta$ is the identity of $G_\beta$, then $ae_\beta = a\phi_{\alpha,\alpha\beta}$, and since the linking homomorphisms are one-to-one, $(a, b) \notin \sigma$, so that (iii) holds. $S$ is in fact the subdirect product of $Y$ and $\varinjlim G_\alpha$.

Similarly, one can obtain a global characterization of commutative semisimple semigroups as follows. A commutative semigroup $S$ is semisimple if and only if it can be embedded in the direct product of a semilattice and a semisimple group.

In general the converse of Theorem 2 does not hold without additional assumptions, even in the case where each $S_\alpha$ is a group. Jordan has given a converse of Theorem 2 for $H$-semigroups that are inverse semigroups or periodic in [6, Theorem 3] and [7, Theorem 5], respectively, by assuming the existence of a collection of subsemigroups with certain properties. In each case the semisimple semigroups are necessarily semilattices of abelian groups, hence a special case of Theorem 2. For the periodic case the following corollary sharpens Theorem 5 of [7] by eliminating the extra condition to give a converse of Theorem 2.

**Corollary 4.** *Let $S$ be a periodic semigroup which is a semilattice of semisimple abelian groups $G_\alpha$, $\alpha \in Y$, such that the multiplication homomorphisms are one-to-one, then $S$ is semisimple.*

**Proof.** Each $G_\alpha$ is periodic abelian and semisimple so its $p$-primary components are elementary abelian for each prime $p$. It follows that the $p$-primary components of $\varinjlim G_\alpha$ are elementary, so $\varinjlim G_\alpha$ is semisimple and hence so is $S$.

Another finiteness condition that yields a converse for a semilattice of groups is that the semilattice $Y$ has a zero. (See [7, Corollary 5.5].)

**Corollary 5.** *Let the semigroup $S$ be a semilattice of semisimple abelian groups $G_\alpha$, $\alpha \in Y$, where $Y$ has a zero, and such that the multiplication homomorphisms are one-to-one, then $S$ is semisimple.*

**Proof.** In this case $\varinjlim G_\alpha$ is isomorphic to $G_0$ which is semisimple, and the semisimplicity of $S$ follows.

We now turn our attention to the other possibility for the subsemigroups $S_\alpha$, a commutative, cancellative, archimedean semigroup without idempotent, or $N$-semigroup. Examples of such semigroups are the positive integers, positive rationals and positive reals under addition. Tamura [11] has given the following characterization of $N$-semigroups. Let $N$ denote the set of nonnegative integers and let $G$ be any abelian group. Let $I$ be a mapping from $G \times G$ to $N$ satisfying:

    (i) $I(a, b) = I(b, a)$, $a, b \in G$,

    (ii) $I(a, b) + I(ab, c) = I(a, bc) + I(b, c)$, $a, b, c \in G$,

(iii) for $a \in G$, $I(a^m, a) > 0$ for some $m > 0$,

(iv) $I(e, e) = 1$ where $e$ is the identity of $G$.

Denote by $(G, I)$ the set $N \times G$ with the binary operation $(m, a)(n, b) = (m + n + I(a, b), ab)$. Then $(G, I)$ is an $N$-semigroup, and every $N$-semigroup is obtained in this manner. We note that neither $G$ nor $I$ is uniquely determined by $S$.

If $S = (G, I)$ is an $N$-semigroup then its maximal modular congruences must all be of type (i) since it is archimedean. Hall [4] has characterized homomorphisms of an $N$-semigroup into an abelian group $G'$ as follows. Let $\phi$ be any mapping from $G$ into $G'$ satisfying

(1) $$(a\phi)(b\phi) = (e\phi)^{I(a,b)}(ab)\phi, \qquad a, b \in G.$$

Define $\theta_\phi$ from $S$ into $G'$ by

(2) $$(m, a)\theta_\phi = (e\phi)^m(a\phi).$$

Then $\theta_\phi$ is a homomorphism of $S$ into $G'$, and every homomorphism is of this type. Thus, to characterize maximal congruences on $N$-semigroups, and thereby the semisimple $N$-semigroups, we need to determine the existence of mappings satisfying (1) onto a cyclic group of prime order. In general this is difficult without additional assumptions on either $G$ or $I$. Note that a mapping $\phi$ satisfying (1) will be a group homomorphism if and only if $e\phi = e'$, the identity of $G'$. Otherwise, $e\phi$ will be a generator of $G'$ since it is of prime order. It is the latter case that is our primary interest since the homomorphism theory is well known. For $S = (G, I)$ and $a \in G$ with $|a| = m$, the order of $a$, we denote $I(a) = \sum_{k=1}^{m} I(a, a^k)$.

**Theorem 6.** Let $S = (G, I)$ with $G$ generated by $a$ and let $G'$ be a group of order $p$, a prime. There exists a mapping $\phi$ from $G$ onto $G'$ satisfying (1) which is not a homomorphism except for the case where $G$ is finite, $p$ divides $|G|$, and $p$ does not divide $I(a)$. The value of $e\phi$ in $G'$ is arbitrary $(\neq e')$. If $G$ is finite and $p$ does not divide $|G|$ then $a\phi$ is uniquely determined by $e\phi$, otherwise it may also be chosen arbitrarily.

**Proof.** If $G$ is infinite cyclic, then let $e\phi = g \neq e'$ in $G'$ and let $a\phi = g^i$ for some $1 \leq i \leq p$. Inductively we define for $n > 1$,

(3) $$a^n\phi = g^{k(n)}, \quad \text{where} \quad k(n) = ni - \sum_{j=1}^{n-1} I(a, a^j),$$

and $a^{-1}\phi = g^k$, where $k \equiv I(a, a^{-1}) - i + 1 \pmod{p}$ and hence is uniquely

determined modulo $p$ given $i$. If $G$ has order $n$, then using (3) we see that $a^n\phi = e\phi$ if and only if

(4)                                        $ni \equiv I(a) \pmod{p}$.

Obviously $(n, p) = 1$ implies a unique solution $i$, while $(n, p) = p = (I(a), p)$ implies $i$ may be chosen arbitrarily. No solution exists in the single case of the hypotheses. To check (1) for any two elements $a^k$, $a^j$ in $G$, the conditions on the exponents of $g$ give equality if and only if

$$I(a^k, a^j) \equiv \sum_{r=1}^{k+j-1} I(a, a^r) - \sum_{r=1}^{k-1} I(a, a^r) - \sum_{r=1}^{j-1} I(a, a^r) \pmod{p}.$$

From Lemma 2 of [2],

$$I(a^k, a^j) = I(a, a^{k+j-1}) + \sum_{r=0}^{k-2} I(a, a^{j+r}) - \sum_{r=0}^{k-2} I(a, a^{k-1-r}),$$

which is easily seen to be equal to the right side of the congruence, so this congruence holds for all $p$, and (1) is satisfied if $G$ is infinite or $j + k \le n$. If $j + k > n$ then $j + k - n = t < n$ when $G$ is finite of order $n$, and $a^{j+k} = a^t$. Then (4) gives

$$(j + k - t)i \equiv ni \equiv \sum_{r=1}^{n} I(a, a^r) \equiv \sum_{r=t}^{j+k-t-1} I(a, a^r),$$

so that $a^{j+k}\phi = a^t\phi$ and (1) holds in this case as well.

The next result allows us to extend our definition of $\phi$ to a large class of groups.

**Theorem 7.** *Let* $S = (G, I)$ *where* $G$ *is the direct product* $H \times K$. *Assume* $\phi_1$ *and* $\phi_2$ *are defined on* $H$ *and* $K$ *respectively to satisfy* (1) *such that* $e\phi_1 = e\phi_2$. *Set* $e\phi = e\phi_1$ *and for* $hk \in G$ *define* $(hk)\phi = (e\phi)^{-I(h,k)}(h\phi_1)(k\phi_2)$, *then* $\phi$ *satisfies* (1) *on* $G$.

**Proof.** Let $x = ab$ and $y = cd$ be elements of $G$, where $a, c \in H$ and $b, d \in K$. Then

$$(x\phi)(y\phi) = (e\phi)^{-I(a,b)-I(c,d)}(a\phi_1)(b\phi_2)(c\phi_1)(d\phi_2)$$

and

$$(xy)\phi = (acbd)\phi = (e\phi)^{-I(ac,bd)}(ac)\phi_1(bd)\phi_2$$

$$= (e\phi)^{-I(ac,bd)-I(a,c)-I(b,d)}(a\phi_1)(c\phi_1)(b\phi_2)(d\phi_2).$$

Multiplying $(xy)\phi$ by $(e\phi)^{l(x,y)}$ makes the exponent of $e\phi$ equal to $l(ab, cd) - l(ac, bd) - l(a, c) - l(b, d)$. By Lemma 6 of [2], this is equal to $- l(a, b) - l(c, d)$, so (1) is satisfied.

If $G$ is semisimple then there are lots of maximal congruences on $G$ and it is natural to expect a relationship to the semisimplicity of $S = (G, l)$. The next result shows that this is the case at least when $G$ is finitely generated.

**Theorem 8.** *Let $S = (G, l)$ where $G$ is a finitely generated semisimple abelian group, then $S$ is semisimple.*

**Proof.** If $(m, a)$ and $(n, b)$ are two elements of $S$ with $a \neq b$ then any homomorphism $\phi$ separating $a$ and $b$ will give a homomorphism $\theta_\phi$ separating $(m, a)$ and $(n, b)$. Thus consider $(m, a) \neq (n, a)$ in $S$ and write $G = \prod_{k=1}^{t} G_k$ where $G_k = \langle a_k \rangle$. Let $p$ be a prime such that $(p, m - n) = (p, |G_k|) = (p, l(a_k)) = 1$ for $k = 1, \dots, t$. By Theorems 6 and 7 we can define a mapping $\phi$ which is not a homomorphism from $G$ onto a cyclic group $G'$ of order $p$. Further, $(m, a)\theta_\phi \neq (n, a)\theta_\phi$ since $(p, m - n) = 1$, so $S$ is semisimple.

If $G$ is any abelian group and we define $l(a, b) = 1$ for all $a, b$ in $G$, then $S = (G, l)$ is an $N$-semigroup. These $N$-semigroups are of interest since they give lots of examples, are relatively easy to study, and they turn out to be fundamental in a sense to the general theory. For this class we are able to obtain a converse to Theorem 8, though it is not true in general.

**Theorem 9.** *Let $S = (G, l)$ be an $N$-semigroup with $G$ finitely generated or periodic and $l(a, b) = 1$ for all $a, b$ in $G$. If $S$ is semisimple, then $G$ is semisimple.*

**Proof.** The torsion subgroup of $G$ is the direct product of $p$-primary subgroups $G_p$. Let $a \in G_p$ with $|a| = p^n$, $n \geq 1$. If $n > 1$ then $a \neq a^{p+1}$ so there is a homomorphism $\theta_\phi$ onto a group $G'$ of prime order $q$ separating $(0, a)$ and $(0, a^{p+1})$. Thus $a\phi = (0, a)\theta_\phi \neq (0, a^{p+1})\theta_\phi = a^{p+1}\phi$ so that $\phi$ is not a homomorphism. Since (1) holds, $e\phi = g$ is not the identity of $G'$ and must therefore generate $G'$. Letting $a\phi = g^i$, $1 \leq i \leq q$, we have $a^k\phi = g^{ki-k+1}$ for all $k \in N$ by induction. If $q \neq p$ then $g = e\phi = a^{p^n}\phi = g^{p^n i - p^n + 1}$ implies $p^n i - p^n + 1 \equiv 1 \pmod{q}$ so $i \equiv 1 \pmod{q}$. But then $i = 1$ so $a\phi = a^{p+1}\phi$, a contradiction. On the other hand, if $q = p$, then $i \equiv (p + 1)i - (p + 1) + 1 \pmod{p}$ gives $a\phi = a^{p+1}\phi$ again. We conclude that $n = 1$, so $G_p$ is elementary abelian and $G$ is semisimple.

A general characterization of semisimple $N$-semigroups appears to be

quite complicated due to two factors. First is the complicated structure of $G$ itself when it is not torsion or finitely generated. Secondly, the conditions on the function $I$ are quite general so that large numbers of them exist and not much can be said about them [2]. For this reason, the conditions for semisimplicity turn out to be number theoretical restrictions on $I$. We conclude with a characterization for the two cases where $G$ is finitely generated or $\sigma(\rho^\infty)$ for some prime $p$.

**Theorem 10.** *Let $S = (G, I)$ where $G$ is finitely generated abelian with torsion subgroup $\Pi_{k=1}^s G_k$, $G_k = \langle a_k \rangle$ of order $r_k = p_k^{s_k}$ and $\Pi_{k=1}^s r_k = M$. For each $k$, let $M_k = M/r_k$ and $I_k = I(a_k)$. Then $S$ is semisimple if and only if given any collection of integers $l_k$, $k = 1, \ldots, s$, satisfying $|l_k| \le s_k$ and $l_k \equiv 0 \pmod{p_k}$, if $\Sigma_{k=1}^s l_k M_k I_k = Mz$ for some $z \in N$, then there exist a prime $p$ and some collection $i_k$ satisfying $r_k i_k \equiv I_k \pmod p$, $k = 1, \ldots, s$, such that $z \not\equiv \Sigma_{k=1}^s l_k i_k \pmod p$.*

**Proof.** Let $(m, x)$ and $(n, y)$ be distinct elements of $S$. A homomorphism $\theta_\phi$ of $S$ onto a cyclic group of prime order where $\phi$ is also a homomorphism will separate $(m, x)$ and $(n, y)$ if and only if $\phi$ separates $x$ and $y$. Thus if $x = \Pi a_k^{m_k} u$ and $y = \Pi a_k^{n_k} v$, where $u, v$ are from the torsion free part of $G$, are not separated by a maximal group homomorphism, then we may assume $u = v$ and $p_k | (m_k - n_k)$, $k = 1, \ldots, s$. If $\phi$ satisfies (1) and is not a homomorphism then $e\phi = g \ne e'$ and $a_k \phi = g^{i_k}$ where $i_k$ satisfies $r_k i_k \equiv I_k \pmod p$ by (4). From (2) and (3) we get $(m, x)\theta_\phi$ is the element $g$ raised to the power $m + \Sigma_{k=1}^s m_k i_k + F_x$ where $F_x$ is an integer depending only on $x$. Thus $(m, x)\theta_\phi = (n, y)\theta_\phi$ if and only if

$$(5) \qquad m - n \equiv \sum_{k=1}^s (n_k - m_k) i_k + F_y - F_x \pmod p.$$

Set $l_k = m_k - n_k$ and assume $M \nmid \Sigma_{k=1}^s l_k M_k I_k$. The terms of the summation depend only on $x$ and $y$, so for any $m, n$ we must have $M(m - n) \ne \Sigma l_k M_k I_k + M(F_y - F_x)$. Thus we can choose a prime $p \nmid M$ so that the conditions of Theorem 6 hold for each $G_k$, there are unique solutions $i_k$ to $r_k i_k \equiv I_k \pmod p$, and $M(m - n) \not\equiv \Sigma l_k M_k I_k + M(F_y - F_x) \pmod p$. $M = r_k M_k$ and $I_k \equiv r_k i_k \pmod p$ imply $M(m - n) \not\equiv \Sigma M l_k i_k + M(F_y - F_x) \pmod p$, and since $(M, p) = 1$, (5) cannot hold. If on the other hand, $\Sigma l_k M_k I_k = Mz$ for some

integer $z$ then $M$ divides $\Sigma l_k M_k I_k + M(F_y - F_x)$. The above argument will work to give separation of $(m, x)$ and $(n, y)$ except when $m$ and $n$ satisfy $m - n = z + F_y - F_x$. Now (5) fails for such a pair $m$, $n$ if and only if $z \not\equiv \Sigma l_k i_k \pmod p$ which is the condition of the theorem.

**Theorem 11.** *Let $G = \sigma(p^\infty)$ for some prime $p$ and $S = (G, I)$ for some index function $I$. $G = \langle a_1, a_2, a_3, \ldots \rangle$, where $a_1^p = e$ and $a_n^p = a_{n-1}$ for $n > 1$. Let $I_n = I(a_n)$. Then $S$ maps homomorphically onto a group of order $q$ for every prime $q \neq p$. Further, $S$ maps onto a group of order $p$ if and only if $p$ divides $I_1$.*

**Proof.** If $q \neq p$ and $G_n = \langle a_n \rangle$ then Theorem 6 gives a unique $i_n$ satisfying (4) and we define $a_n \phi = g^{i_n}$ where $\langle g \rangle = G'$ of order $q$. This is well defined on $G$ if and only if $a_n \phi = (a_{n+1}^p)\phi$. Using (3) and letting $K_n = \Sigma_{j=1}^{p-1} I(a_{n+1}, a_{n+1}^j)$, we get equality if and only if $i_n \equiv p i_{n+1} - K_n \pmod q$ for all $n$. Since $p \neq q$, this holds if and only if

$$p^n i_n \equiv p^{n+1} i_{n+1} - p^n K_n \pmod q \Longleftrightarrow I_n \equiv I_{n+1} - p^n K_n \pmod q.$$

Substituting $a_n = a_{n+1}^p$ in $I_n$, the last congruence is

$$\sum_{j=1}^{p^n} I(a_{n+1}^p, a_{n+1}^{pj}) \equiv I_{n+1} - p^n K_n \pmod q.$$

We now claim that we actually have equality in this last expression, that is, simplifying the notation a little, if $a \in G$ has order $p^{n+1}$, then

$$\sum_{j=1}^{p^n} I(a^p, a^{pj}) = \sum_{j=1}^{p^{n+1}} I(a, a^j) - p^n \sum_{j=1}^{p-1} I(a, a^j).$$

From Lemma 2 of [2] we have

$$I(a^p, a^{pj}) = I(a, a^{p+pj-1}) + \sum_{k=0}^{p-2} I(a, a^{pj+k}) - \sum_{k=0}^{p-2} I(a, a^{p-1-k}).$$

Simplifying gives

$$\sum_{j=1}^{p^n} I(a^p, a^{pj}) = \sum_{j=1}^{p^n} \sum_{k=0}^{p-1} I(a, a^{pj+k}) - p^n \sum_{k=1}^{p-1} I(a, a^k).$$

Using the fact that $a^{p^{n+1}} = e$, the first expression on the right becomes

$\sum_{j=1}^{p^{n+1}} I(a, a^j)$ and our claim is proved. This implies $\phi$ is well defined and so a homomorphism onto $G'$ exists. In particular we note that the above equality implies

(6)                          $I_n = I_{n+1} - p^n K_n$    for all $n$.

If $q = p$ then Theorem 6 requires $I_n \equiv 0 \pmod{p}$ for all $n$ and $i_n$ is arbitrary. However $\phi$ is well defined if and only if $i_n \equiv -K_n \pmod{p}$ which has a unique solution for each $n$, giving the mapping $\theta_\phi$ and conversely. Finally, (6) says $I_n \equiv 0 \pmod{p}$ for all $n$ if and only if $p$ divides $I_1$.

**Corollary 12.** $p^n$ divides $I_n$ if and only if $p^n$ divides $I_{n+1}$ for all positive integers $n$.

**Theorem 13.** Let $G = \sigma(p^\infty)$ for some prime $p$ and $S = (G, I)$ for some index function $I$. $G = \langle a_1, a_2, \ldots \rangle$ where $a_1^p = e$ and $a_n^p = a_{n-1}$ for $n > 1$. Let $I_n = I(a_n)$. Then $S$ is semisimple if and only if for each positive integer $n$, given $u$ such that $1 \le u < p^n$, if $p^n$ divides $uI_n$, then $p^{n+1}$ does not divide $uI_{n+1}$.

**Proof.** Let $(t, x)$, $(s, y)$ be distinct elements of $S$, then for some minimal $n$ we have $x = a_n^j$, $y = a_n^k$, where (say) $j \ge k$. If $j = k$ then $t \ne s$ and to separate these two elements by (3) we need only satisfy $t - s \not\equiv 0 \pmod{q}$ which is possible by Theorem 11. Thus assume $j \ne k$. Again using (3), we are able to separate $(t, x)$ and $(s, y)$ if and only if there exists a prime $q$ such that

(7)                    $(j - k)i_n \not\equiv t - s + \sum_{r=k}^{j-1} I(a_n, a_n^r) \pmod{q}$.

If $p^n$ does not divide $(j - k)I_n$, then $(j - k)I_n \ne p^n(t - s) + p^n \sum_{r=k}^{j-1} I(a_n, a_n^r)$ for any $t$ and $s$, so there exists a prime $q \ne p$ such that

$$(j - k)I_n \not\equiv p^n(t - s) + p^n \sum_{r=k}^{j-1} I(a_n, a_n^r) \pmod{q}.$$

Choosing $i_n$ to satisfy (4) gives

$$(j - k)p^n i_n \not\equiv p^n(t - s) + p^n \sum_{r=k}^{j-1} I(a_n, a_n^r) \pmod{q},$$

and since $q \ne p$; (7) holds. If, on the other hand, $(j - k)I_n = p^n z$ for some integer $z$, then we obtain separation as above except for those integers $t$, $s$

such that $(j - k)I_n = p^n(t - s) + p^n \sum_{r=k}^{j-1} I(a_n, a_n^r)$, that is, $z = t - s + \sum_{r=k}^{j-1} I(a_n, a_n^r)$. It follows that we can separate $(t, x)$ and $(s, y)$ for such $t$, $s$ if and only if there exist a prime $q$ and $i_n$ satisfying (4) such that $(j - k)i_n \not\equiv z \pmod{q}$. We show that $q$ must equal $p$. Obviously $(j - k)I_n \equiv p^n z \pmod{q}$ for every prime $q$, and if $q \neq p$, then $z \equiv (p^n)^{-1}(j - k)I_n \pmod{q}$. If $i_n$ satisfies (4), that is $p^n i_n \equiv I_n \pmod{q}$, then $(j - k)i_n \equiv (j - k)(p^n)^{-1}I_n \equiv z \pmod{q}$, so we must choose $q = p$. Since $j - k < p^n$ and $(j - k)I_n = p^n z$ we must have $p|I_n$ so $S$ maps homomorphically onto a group of order $p$ by Theorem 11. From the proof of Theorem 11 we observe $i_n \equiv -K_n \pmod{p}$, so we get separation if and only if $-(j - k)K_n \not\equiv z \pmod{p}$ or $z + (j - k)K_n \not\equiv 0 \pmod{p}$. Now $p^n z = (j - k)I_n = (j - k)I_{n+1} - (j - k)p^n K_n$ by (6) so $(j - k)I_{n+1} = p^n(z + (j - k)K_n)$. From this equation, $z + (j - k)K_n \equiv 0 \pmod{p}$ if and only if $p^{n+1}$ divides $(j - k)I_{n+1}$, proving the theorem.

### REFERENCES

1. B. D. Arendt, *Semisimple bands*, Trans. Amer. Math. Soc. 143 (1969), 133–143. MR 40 #255.

2. R. G. Biggs, M. Sasaki and T. Tamura, *Non-negative integer valued functions on commutative groups*. I, Proc. Japan Acad. 41 (1965), 564–569. MR 33 #2721.

3. A. H. Clifford, *Radicals in semigroups*, Semigroup Forum 1 (1970), no. 2, 103–127. MR 42 #1922.

4. R. E. Hall, *The translational hull of an N-semigroup*, Pacific J. Math. 41 (1972), 379–389.

5. H.-J. Hoehnke, *Structure of semigroups*, Canad. J. Math. 18 (1966), 449–491. MR 33 #5762.

6. M. J. Jordan, S.C., *Inverse H-semigroups, and t-semisimple inverse H-semigroups*, Trans. Amer. Math. Soc. 163 (1972), 75–84.

7. ———, *Periodic H-semigroups, and t-semisimple periodic H-semigroups*, Pacific J. Math. 41 (1972), 437–446. MR 46 #5498.

8. D. R. LaTorre, *Modular congruences and the Brown-McCoy radical for semigroups*, Proc. Amer. Math. Soc. 29 (1971), 427–433. MR 43 #6350.

9. R. H. Oehmke, *On maximal congruences and finite semisimple semigroups*, Trans. Amer. Math. Soc. 125 (1966), 223–237. MR 34 #2739.

10. M. Petrich, *Introduction to semigroups*, Merrill, Columbus, Ohio, 1973.

11. T. Tamura, *Commutative nonpotent archimedean semigroup with cancellation law*. I, J. Gakugei Tokushima Univ. 8 (1957), 5–11. MR 20 #3224.

12. T. Tamura and N. Kimura, *On decompositions of a commutative semigroup*, Kōdai Math. Sem. Rep. 4 (1954), 109–112. MR 16, 670.

13. R. Yoshida, *Ideal extensions of semigroups and compound semigroups*, Mem. Res. Inst. Sci. Eng. Ritumeiken Univ. 13 (1965), 1–8.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MISSOURI, COLUMBIA, MISSOURI 65201