SUBDIRECTLY IRREDUCIBLE SEMIGROUPS

THESIS

Presented to the Graduate Council of the
North Texas State University in Partial
Fulfillment of the Requirements

For the Degree of

MASTER OF ARTS

By

Richard Alan Winton, B. S.
Denton, Texas

December, 1978

TABLE OF CONTENTS

CHAPTER I

GENERAL PROPERTIES OF SEMIGROUPS

Definition 1.1. The ordered pair $(S,*)$ is a semigroup iff S is a set and $*$ is an associative binary operation (multiplication) on S.

Notation. A semigroup $(S,*)$ will ordinarily be referred to by the set S, with the multiplication understood. In other words, if $(a,b) \in S \times S$, then $*[(a,b)] = a*b = ab$.

The proof of the following proposition is found on p. 4 of Introduction to Semigroups, by Mario Petrich.

Proposition 1.2. Every semigroup S satisfies the general associative law.

Proof. If $\{a_i\}_{i=1}^{n} \subseteq S$, then define $a_1 a_2 \cdots a_n \equiv a_1(a_2(\cdots(a_{n-1}a_n)\cdots))$. If $a \in S$ and a is the product of one element $a_1 \in S$, then $a = a_1$, and the product does not depend on the positioning of parentheses. Now suppose the general associative law holds for all products of r elements, where $r < n$. If a is the product of n elements of S, then there exists $r \in Z^+$, $1 \leq r \leq n$, such that

$$\begin{aligned} a &= (a_1 a_2 \cdots a_r)(a_{r+1} a_{r+2} \cdots a_n) \\ &= [a_1(a_2 \cdots a_r)](a_{r+1} \cdots a_n) \\ &= a_1[(a_2 \cdots a_r)(a_{r+1} \cdots a_n)] \end{aligned}$$

$$= a_1(a_2 \cdots a_r \cdot a_{r+1} \cdots a_n)$$
$$= a_1 a_2 \cdots a_n.$$

Thus by induction, S satisfies the general associative law, and so all parentheses may be omitted from products of elements of a semigroup.

Definition 1.3. A nonempty subset T of a semigroup S is a subsemigroup of S iff T is closed under the operation on S (if $a,b \varepsilon T$, then $ab \varepsilon T$).

Thus a subsemigroup T of a semigroup S, along with the multiplication of S, is itself a semigroup since associativity is inherited from S.

Definition 1.4. A semigroup S is generated by a subset G of S iff every element of S can be expressed as the product of elements of G.

Definition 1.5. A semigroup S is cyclic iff there exists $a \varepsilon S$ such that S is generated by $\{a\}$.

Definition 1.6. If A is a nonempty subset of a semigroup S, then the subsemigroup of S generated by

A is $\{a_1 a_2 \cdots a_n \mid a_i \varepsilon A,\ 1 \leq i \leq n;\ n \varepsilon Z^+\}$, where Z^+ is the set of all positive integers.

Lemma 1.7. If A is a nonempty subset of a semigroup S, then the subsemigroup of S generated by A is the intersection of all subsemigroups of S containing A.

Proof. Let $T \equiv \{\prod_{i=1}^{n} a_i \mid n \varepsilon Z^+;\ a_i \varepsilon A,\ 1 \leq i \leq n\}$, and let $\{G_\alpha\}_{\alpha \varepsilon \Gamma} \equiv \{G \text{ subsemigroup of } S \mid A \subseteq G\}$.

If $\prod_{i=1}^{n} a_i \varepsilon T$, then $a_i \varepsilon A$ for each i, $1 \leq i \leq n$. Therefore, since $A \subseteq G_\alpha$ for all $\alpha\varepsilon\Gamma$, then for each i, $1 \leq i \leq n$, $a_i \varepsilon G_\alpha$ for all $\alpha\varepsilon\Gamma$.

Therefore, $\prod_{i=1}^{n} a_i \varepsilon G_\alpha$ for all $\alpha\varepsilon\Gamma$, so that $\prod_{i=1}^{n} a_i \varepsilon \bigcap_{\alpha\varepsilon\Gamma} G_\alpha$. Thus $T \subseteq \bigcap_{\alpha\varepsilon\Gamma} G_\alpha$. However, T itself is a subsemigroup of S and obviously contains A. Therefore, $T \varepsilon \{G_\alpha\}_{\alpha\varepsilon\Gamma}$, so that $\bigcap_{\alpha\varepsilon\Gamma} G_\alpha \subseteq T$, and hence $T = \bigcap_{\alpha\varepsilon\Gamma} G_\alpha$.

Definition 1.8. A nonempty subset T of a semigroup S is a left ideal of S iff $a\varepsilon S$, $b\varepsilon T$ imply $ab\varepsilon T$. T is a right ideal of S iff $a\varepsilon S$, $b\varepsilon T$ imply $ba\varepsilon T$. T is a two-sided ideal (or simply an ideal) of S iff T is both a left and right ideal of S. T is a proper ideal of S iff T is an ideal of S and $T \neq S$.

Notation. If $\{A_i\}_{i=1}^{n}$ is a collection of nonempty subsets of a semigroup S, then

$$A_1A_2\cdots A_n = \{a_1\cdot a_2\cdots a_n \mid a_i\varepsilon A_i,\ 1\leq i\leq n\}.$$

If $A_i = \{a\}$, then $A_1A_2\cdots A_{i-1}\, a\, A_{i+1}\cdots A_n = A_1A_2\cdots A_n$. If $A_1 = A_2 = \cdots = A_n = A$, then $A^n = A_1A_2\cdots A_n$. In general, no distinction will be made between an element a of a semigroup S and the singleton set $\{a\}$.

In view of this notation, a nonempty subset T of a semigroup S is: (i) a subsemigroup of S iff $T^2 \subseteq T$, (ii) a left ideal of S iff $ST \subseteq T$, (iii) a right ideal of S iff $TS \subseteq T$, (iv) an ideal of S iff $ST \cup TS \subseteq T$. Also, if A is a nonempty subset of S, then the subsemigroup of S generated by A is $\bigcup_{i=1}^{\infty} A^n$.

Lemma 1.9. Each of the collections (a) of all left ideals, (b) all right ideals, (c) all ideals of a semigroup S is closed under (i) arbitrary intersection, if nonempty, (ii) arbitrary union. Also, the collection of all ideals is closed under finite intersection.

Proof. Part I: Let $\{G_\alpha\}_{\alpha\varepsilon A}$ be a collection of left ideals of a semigroup S such that $\bigcap_{\alpha\varepsilon A} G_\alpha \neq \phi$. If $x\varepsilon S$, $y\varepsilon \bigcap_{\alpha\varepsilon A} G_\alpha$, then $y\varepsilon G_\alpha$ for each $\alpha\varepsilon A$. Since G_α is a left ideal of S, then $xy\,\varepsilon\, G_\alpha$ for each $\alpha\varepsilon A$, so that $xy\,\varepsilon \bigcap_{\alpha\varepsilon A} G_\alpha$. Therefore $\bigcap_{\alpha\varepsilon A} G_\alpha$ is a left ideal of S. Similarly, if $\{G_\alpha\}_{\alpha\varepsilon A}$ is a collection of right ideals (or ideals) of S such that $\bigcap_{\alpha\varepsilon A} G_\alpha \neq \phi$, then $\bigcap_{\alpha\varepsilon A} G_\alpha$ is a right ideal (or ideal) of S.

Part II: If $\{G_\alpha\}_{\alpha\varepsilon A}$ is a collection of left ideals of S, then for each $\alpha\varepsilon A$, $G_\alpha \neq \phi$, so that $\bigcup_{\alpha\varepsilon A} G_\alpha \neq \phi$. Furthermore, if $x\varepsilon S$ and $y\varepsilon \bigcup_{\alpha\varepsilon A} G_\alpha$, then there exists $\beta\varepsilon A$ such that $y\varepsilon G_\beta$. Therefore $xy\,\varepsilon\, G_\beta \subseteq \bigcup_{\alpha\varepsilon A} G_\alpha$, and so $\bigcup_{\alpha\varepsilon A} G_\alpha$ is a left ideal of S. Similarly, if $\{G_\alpha\}_{\alpha\varepsilon A}$ is a collection of right ideals (or ideals) of S, then $\bigcup_{\alpha\varepsilon A} G_\alpha$ is a right ideal (or ideal) of S.

Part III: If A and B are ideals of a semigroup S, then $A \neq \phi$ and $B \neq \phi$, so there exist $x\varepsilon A$, $y\varepsilon B$. Therefore $xy\,\varepsilon\, A$ and $xy\,\varepsilon\, B$, so that $xy\,\varepsilon\, A\cap B$ and thus $A\cap B \neq \phi$. Furthermore, if $p\varepsilon A\cap B$ and $q\varepsilon S$, then $p\varepsilon A$ and $p\varepsilon B$. Therefore $pq, qp\,\varepsilon\, A$ and $pq, qp\,\varepsilon\, B$, so that $pq, qp\,\varepsilon\, A\cap B$. Thus $A\cap B$ is is an ideal of S. Now suppose that if $\{A_i\}_{i=1}^{k}$ is a collection of ideals in S, then $\bigcap_{i=1}^{k} A_i$ is an ideal in S. Therefore, if $\{A_i\}_{i=1}^{k+1}$ is a collection of ideals of S, then $\bigcap_{i=1}^{k} A_i$ is an ideal of S. But then $\bigcap_{i=1}^{k+1} A_i = \bigcap_{i=1}^{k} A_i \cap A_{k+1}$ is an ideal of S since the case for two ideals was already proven. Therefore, by induction, for each $n \varepsilon Z^+$, if $\{A_i\}_{i=1}^{n}$ is a collection of ideals of S, then $\bigcap_{i=1}^{n} A_i$ is an ideal of S.

Definition 1.10. If S is a semigroup, $A \subseteq S$, and $A \neq \phi$, then the left ideal generated by A is $L_A = \bigcap\{T$ left ideal of $S | A \subseteq T\}$. A left ideal of S generated by a singleton subset $\{a\}$ of S is the principal left ideal of S generated by a, and will be denoted by L(a). Corresponding definitions are valid for right ideals with notation R_A, R(a), and ideals with notation J_A, J(a).

Lemma 1.11. If S is a semigroup and $a \varepsilon S$, then
(1) $L(a) = \{a\} \cup Sa$, (2) $R(a) = \{a\} \cup aS$, and
(3) $J(a) = \{a\} \cup aS \cup Sa \cup SaS$.

Proof. Part I: Let $\{G\alpha\}_{\alpha \varepsilon A}$ be the collection of all left ideals of S containing a, so that $L(a) = \bigcap_{\alpha \varepsilon A} G\alpha$.
(i) Since $a \varepsilon G\alpha$ for each $\alpha \varepsilon A$, then $a \varepsilon \bigcap_{\alpha \varepsilon A} G\alpha = L(a)$, so that $\{a\} \subseteq L(a)$. (ii) Since L(a) is a left ideal of S and $a \varepsilon L(a)$, then for each $x \varepsilon S$, $xa \varepsilon L(a)$ so that $Sa \subseteq L(a)$. Therefore, by (i), (ii), $\{a\} \cup Sa \subseteq L(a)$.

Let $x \varepsilon S$, $y \varepsilon \{a\} \cup Sa$, so that either $y = a$ or $y = ka$ for some $k \varepsilon S$.

(i) If $y = a$, then $xy = xa \in Sa \subseteq \{a\} \cup Sa$.

(ii) If $y = ka$, then $xy = x(ka) = (xk)a \in Sa \subseteq \{a\} \cup Sa$, since $xk \in S$.

Therefore $\{a\} \cup Sa$ is a left ideal of S and contains a, so that $\{a\} \cup Sa \in \{G_\alpha\}_{\alpha \in A}$, and so $L(a) = \bigcap_{\alpha \in A} G_\alpha \subseteq \{a\} \cup Sa$.

Part II: Similarly, $R(a) = \{a\} \cup aS$.

Part III: Let $\{H_\alpha\}_{\alpha \in A}$ be the collection of all ideals of S containing a, so that $J(a) = \bigcap_{\alpha \in A} H_\alpha$.

(i) Since $a \in H_\alpha$ for each $\alpha \in A$, then $a \in \bigcap_{\alpha \in A} H_\alpha = J(a)$, so that $\{a\} \subseteq J(a)$.

(ii) Since $J(a)$ is an ideal of S and $a \in J(a)$, then for each $x \in S$, $ax \in J(a)$ and $xa \in J(a)$, so that $aS \subseteq J(a)$ and $Sa \subseteq J(a)$.

(iii) Also, if $x, y \in S$, then $xa \in J(a)$ since $J(a)$ is a left ideal, and so $xay = (xa)y \in J(a)$ since $J(a)$ is a right ideal. Therefore, $SaS \subseteq J(a)$. Thus by (i)-(iii), $\{a\} \cup Sa \cup aS \cup SaS \subseteq J(a)$.

If $x \in S$, $y \in \{a\} \cup Sa \cup aS \cup SaS$, then either $y = a$, $y \in Sa$, $y \in aS$, or $y \in SaS$.

(i) If $y = a$, then $xy = xa \in Sa$ and $yx = ax \in aS$, so that $xy, yx \in \{a\} \cup Sa \cup aS \cup SaS$.

(ii) If $y \in Sa$, then $y = ka$ for some $k \in S$. Therefore, $xy = x(ka) = (xk)a \in Sa$, since $xk \in S$, and $yx = kax \in SaS$, so that $xy, yx \in \{a\} \cup Sa \cup aS \cup SaS$.

(iii) If $y \in aS$, then $y = ak$ for some $k \in S$. Therefore, $xy = xak \in SaS$ and $yx = (ak)x = a(kx) \in aS$, since $kx \in S$, so that $xy, yx \in \{a\} \cup Sa \cup aS \cup SaS$.

(iv) If $y \in SaS$, then $y = paq$ for some $p,q \in S$. Therefore, $xy = x(paq) = (xp)aq \in SaS$ since $xp \in S$, and $yx = (paq)x = pa(qx) \in SaS$ since $qx \in S$, so that $xy, yx \in \{a\} \cup Sa \cup aS \cup SaS$.

Thus, by (i)-(iv), $\{a\} \cup Sa \cup aS \cup SaS$ is an ideal of S and contains a, so that $\{a\} \cup Sa \cup aS \cup SaS \in \{H_\alpha\}_{\alpha \in A}$, and so $J(a) = \bigcap_{\alpha \in A} H_\alpha \subseteq \{a\} \cup Sa \cup aS \cup SaS$.

Definition 1.12. A semigroup S is left (right) simple iff S is the only left (right) ideal of S. S is simple iff S is the only ideal of S.

Lemma 1.13. A semigroup S is left simple iff $Sa = S$ for all $a \in S$. A semigroup S is right simple iff $aS = S$ for all $a \in S$. A semigroup S is simple iff $SaS = S$ for all $a \in S$.

Proof. Part I: Suppose S is left simple and $a \in S$. If $p \in S$ and $q \in Sa$, then $q = ka$ for some $k \in S$, and so $pq = p(ka) = (pk)a \in Sa$ since $pk \in S$. Therefore, Sa is a left ideal of S so that $Sa = S$ since S is left simple. Thus $Sa = S$ for all $a \in S$.

Suppose $Sa = S$ for all $a \in S$. If G is a left ideal of S, then $G \neq \phi$ so that there exists $a \in G$. Therefore, $S = Sa \subseteq SG \subseteq G$ (since G is a left ideal) $\subseteq S$, so that $G = S$. Thus S is left simple.

Part II: Similarly, S is right simple iff $aS = S$ for all $a \in S$.

Part III: Suppose S is simple and $a \in S$. If $p \in S$, $q \in SaS$, then $q = kat$ for some $k,t \in S$. Therefore

$pq = p(kat) = (pk)at \in SaS$ since $pk \in S$, and
$qp = (kat)p = ka(tp) \in SaS$ since $tp \in S$. Thus SaS is an ideal of S, and so $SaS = S$ since S is simple.

Suppose $SaS = S$ for all $a \in S$. If G is an ideal of S, then $G \neq \phi$ so there exists $a \in G$. Therefore if $x, y \in S$, then $xa \in G$ and so $xay = (xa)y \in G$. Thus $S = SaS \subseteq G \subseteq S$ so that $G = S$, and so S is simple.

Definition 1.14. The intersection of all ideals of a semigroup S, if nonempty, is the kernel of S.

Lemma 1.15. If K is a simple ideal of a semigroup S, then K is the kernel of S.

Proof. Suppose K is a simple ideal of a semigroup S. If G is any ideal of S, then $K \cap G$ is an ideal of S by lemma 1.9. Since $K \cap G \subseteq K$, then $K \cap G = K$ since K is simple. Therefore $K = K \cap G \subseteq G$ for each ideal G of S, so that $K \subseteq \bigcap\{G | G$ is an ideal of $S\}$. But $K \in \{G | G$ is an ideal of $S\}$, and so $\bigcap\{G | G$ is an ideal in $S\} \subseteq K$. Thus $K = \bigcap\{G | G$ is an ideal of $S\}$ = kernel of S, since $K \neq \phi$.

Definition 1.16. Let S be a semigroup and let $d \in S$. An element e of S is: (i) a left identity of d iff $ed = d$, (ii) a right identity of d iff $de = d$, (iii) a two-sided identity (or simply an identity) of d iff e is both a left and a right identity of d. Furthermore, e is a left (right) identity of S iff e is a left (right) identity of every element of S; and e is a two-sided identity (or simply an identity) of S iff e is both a left and a right identity of S.

Definition 1.17. An element z of a semigroup S is a left zero of S iff zx = z for all $x \in S$; z is a right zero of S iff xz = z for all $x \in S$; z is a two-sided zero (or simply a zero) of S iff z is both a left and a right zero of S.

Definition 1.18. If S is a semigroup with zero z, then an element p of S is a zero divisor of S iff $p \neq z$ and there exists $q \in S$ such that $q \neq z$ and either pq = z or qp = z.

Notation: If S is a semigroup, an identity 1 may be adjoined to S by defining x1 = 1x = x for all $x \in S$. Similarly, a zero 0 may be adjoined to S by defining x0 = 0x = 0 for all $x \in S$. Let S^1 be the semigroup S with 1 adjoined, and let S^0 be S with 0 adjoined. Thus, according to this notation, if S is a semigroup and $a \in S$, then $L(a) = S^1a$, $R(a) = aS^1$, and $J(a) = S^1aS^1$.

Lemma 1.19. If a semigroup S has an identity, then the identity is unique.

Proof. Suppose e and u are identities for a semigroup S. Then e = eu since u is a right identity, and eu = u since e is a left identity. Thus e = u and the identity is unique.

Lemma 1.20. If a semigroup S has a zero, then the zero is unique.

Proof. Suppose z and w are zeros of a semigroup S. Then z = zw since z is a left zero, and zw = w since w is a right zero. Thus z = w and the zero element is unique.

Notation. If A and B are sets, then (i) $A\backslash B = \{x\varepsilon A | x \notin B\}$, (ii) $|A|$ = cardinality of A, and (iii) if S is a semigroup with 0, then $S^* = S\backslash\{0\}$. Notice that S^* is a semigroup iff S has no zero divisors.

Definition 1.21. A semigroup S in which every element is a left (right) zero is a left (right) zero semigroup. A semigroup S with zero 0 is a zero semigroup iff ab = 0 for all $a,b\varepsilon S$. A semigroup S with zero 0 is 0-simple iff $S^2 \neq \{0\}$ and S has no nonzero proper ideals. Thus S is 0-simple iff S is not a zero semigroup, and the only ideals in S are {0} and S.

Definition 1.22. Elements p and q of a semigroup S commute iff pq = qp.

Definition 1.23. The center of a semigroup S is $C(S) \equiv \{a\varepsilon S | ax = xa \text{ for all } x\varepsilon S\}$.

Definition 1.24. A semigroup S is commutative iff $C(S) = S$.

Definition 1.25. An element x of a semigroup S is idempotent iff $x^2 = x$.

Definition 1.26. A semigroup S is idempotent iff every element of S is idempotent.

Definition 1.27. A semilattice is a commutative idempotent semigroup.

Definition 1.28. A subgroup G of a semigroup S is a subsemigroup of S which is also a group.

The proof of the following proposition is found on p. 10 of Introduction to Semigroups, by Mario Petrich.

Proposition 1.29. If e is an idempotent element of a semigroup S, then

$$G_e \equiv \{a\varepsilon S \mid a = ea = ae,\ e = ab = ba \text{ for some } b\varepsilon S\}$$
$$= \{a\varepsilon S \mid a \ \varepsilon\ eS \cap Se,\ e\ \varepsilon\ aS \cap Sa\}$$

is the greatest subgroup of S having e as its identity.

Proof. Let e be an idempotent element of a semigroup S, and let $G_e \equiv \{a\varepsilon S \mid a = ea = ae,\ e = ab = ba$ for some $b\varepsilon S\}$.

Part I: If $p\ \varepsilon G_e$, then $p = ep\ \varepsilon\ eS$ and $p = pe\ \varepsilon\ Se$, so that $p\ \varepsilon\ eS \cap Se$. Similarly $e = pq\ \varepsilon\ pS$ and $e = qp\ \varepsilon\ Sp$ for some $q\varepsilon S$, so that $e\varepsilon pS \cap Sp$. Therefore, $p\varepsilon \{a\varepsilon S \mid a\varepsilon eS \cap Se,\ e\varepsilon aS \cap Sa\}$, and so $G_e \subseteq \{a\varepsilon S \mid a\ \varepsilon\ eS \cap Se,\ e\ \varepsilon\ aS \cap Sa\}$. Now if $p\ \varepsilon \{a\varepsilon S \mid a\varepsilon eS \cap Se,\ e\varepsilon aS \cap Sa\}$, then there exist $x,y,z,w\ \varepsilon\ S$ such that $p = ex = ye$ and $e = pz = wp$. Since $p = ex$, then $ep = e(ex) = (ee)x = ex = p$, and since $p = ye$ then $pe = (ye)e = y(ee) = ye = p$. Therefore $p = ep = pe$. Furthermore, $eze = (wp)ze = w(pz)e = wee = we$, so that $eze = (ee)ze = e(eze) = e(we) = ewe$, and so $eze = ewe$. Define $q = eze = ewe\ \varepsilon\ S$. Therefore,
$e = ee = (pz)e = p(ze) = (pe)(ze) = p(eze) = pq$ and
$e = ee = e(wp) = (ew)p = (ew)(ep) = (ewe)p = qp$, so that $e = pq = qp$ for $q\varepsilon S$. Thus $p\ \varepsilon\ G_e$, and so $\{a\varepsilon S \mid a\ \varepsilon\ eS \cap Se,\ e\ \varepsilon\ aS \cap Sa\} \subseteq G_e$. Therefore
$G_e \equiv \{a\varepsilon S \mid a = ea = ae,\ e = ab = ba \text{ for some } b\varepsilon S\} =$
$\{a\varepsilon S \mid a\ \varepsilon\ eS \cap Se,\ e\ \varepsilon\ aS \cap Sa\}$.

Part II: (i) If $a,b\ \varepsilon\ G_e$, then $a = ae = ea$, $b = be = eb$, and there exist $p,q\ \varepsilon S$ such that $e = ap = pa = bq = qb$.

Therefore $ab = (ea)b = e(ab)$ and $ab = a(be) = (ab)e$, so that $ab = e(ab) = (ab)e$. Also, since $p, q \in S$, then $qp \in S$. Therefore $(ab)(qp) = [a(bp)]p = (ae)p = ap = e$ and $(qp)(ab) = q[(pa)b] = q(eb) = qb = e$, so that $e = (ab)(qp) = (qp)(ab)$ and $ab \in G_e$. Thus G_e is closed under the multiplication of S.

(ii) G_e inherits associativity from S.

(iii) Since e is idempotent, then $e = ee = ee$ satisfies both equations in the definition of G_e, and so $e \in G_e$. Furthermore, e is identity for G_e by the definition of G_e.

(iv) If $a \in G_e$, then $ae = ea = a$ and $e = ab = ba$ for some $b \in S$, and so $ebe \in S$. Since $ebe = e(ebe) = (ebe)e$ and $e = (ebe)a = a(ebe)$ for $a \in S$, then $ebe \in G_e$ and is inverse for a. Thus G_e is a group with e as its identity.

Part III: Let G be any subgroup of S containing e as its identity. If $p \in G$, then $p = pe = ep$ and there exists $q \in G \subseteq S$ such that $e = pq = qp$, and so $p \in G_e$. Therefore $G \subseteq G_e$ and so G_e is the largest subgroup of S having e as its identity.

<u>Definition 1.30</u>. If S is a semigroup with identity e, then G_e is the group of units of S, and the elements of G_e are the invertible elements of S.

<u>Lemma 1.31</u>. An element x of a semigroup S with identity is invertible iff $xS = Sx = S$.

<u>Proof</u>. Let S be a semigroup with identity e. If $x \in S$ is invertible, then $x = xe = ex$ and $e = xy = yx$ for some $y \in S$.

Therefore, for each $p \varepsilon S$, $p = pe = p(yx) = (py)x \varepsilon Sx$ and $p = ep = (xy)p = x(yp) \varepsilon xS$, so that $S \subseteq Sx$ and $S \subseteq xS$. However, for each $a \varepsilon S$, $ax \varepsilon S$ and $xa \varepsilon S$, so that $Sx \subseteq S$ and $xS \subseteq S$. Therefore $xS = Sx = S$. Conversely, suppose $xS = Sx = S$. Since e is the identity for S, then $S = eS = Se$, so that $x \varepsilon S = S \cap S = eS \cap Se$. Also, $e \varepsilon S = S \cap S = xS \cap Sx$, so that $x \varepsilon \{a \varepsilon S \mid a \varepsilon eS \cap Se,\ e \varepsilon aS \cap Sa\} = G_e$, and thus x is invertible.

<u>Definition 1.32</u>. An element p of a semigroup S is regular iff there exists $x \varepsilon S$ such that $p = pxp$.

<u>Definition 1.33</u>. A semigroup S is regular iff each element of S is regular.

<u>Definition 1.34</u>. Let S be a semigroup and let $p, x \varepsilon S$. Then x is an inverse of p iff $p = pxp$ and $x = xpx$.

<u>Theorem 1.35</u>. In a semigroup S, each regular element p has an inverse which is also regular. Conversely, if an element p of S has an inverse, then both p and its inverse are regular.

<u>Proof</u>. If $p \varepsilon S$ is regular, then there exists $x \varepsilon S$ such that $p = pxp$. Therefore $xpx \varepsilon S$, $p(xpx)p = (pxp)xp = pxp = p$, and $(xpx)p(xpx) = x(pxp)(xpx) = xp(xpx) = x(pxp)x = xpx$. Thus xpx is inverse for p, and since $(xpx)p(xpx) = xpx$ for $p \varepsilon S$, then xpx is regular. Conversely, if $p, x \varepsilon S$ and x is an inverse of p, then $p = pxp$ and $x = xpx$, so that p and x are regular.

<u>Definition 1.36</u>. The order of a finite semigroup S is the number of its elements. If S is not finite, then S is

of infinite order. A semigroup of order one is a trivial semigroup.

<u>Definition 1.37</u>. The order of an element x of a semigroup S is the order of the cyclic subsemigroup of S generated by x.

<u>Definition 1.38</u>. A semigroup S is periodic iff each element of S is of finite order.

CHAPTER BIBLIOGRAPHY

1. Petrich, Mario, Introduction to Semigroups, Columbus, Ohio, Charles E. Merrill Publishing Company, 1973.

CHAPTER II

RELATIONS AND FUNCTIONS ON A SEMIGROUP

Definition 2.1. A binary relation ρ on a set S is a subset of $S \times S$. An alternate notation for $(x,y) \varepsilon \rho$ will be $x \rho y$, in which case x is said to be ρ-related to y. A binary relation ρ on a set S will ordinarily be referred to simply as a relation on S.

Definition 2.2. A relation ρ on a set S is:

(i) reflexive iff $(x,x) \varepsilon \rho$,

(ii) symmetric iff $(x,y) \varepsilon \rho$ implies $(y,x) \varepsilon \rho$,

(iii) antisymmetric iff $(x,y),(y,x) \varepsilon \rho$ implies $x = y$, and

(iv) transitive iff $(x,y),(y,z) \varepsilon \rho$ implies $(x,z) \varepsilon \rho$ for all $x,y,z \varepsilon S$.

Definition 2.3. A relation ρ on a set S is an equivalence relation on S iff ρ is reflexive, symmetric, and transitive.

Definition 2.4. If ρ is an equivalence relation on a set S, then the disjoint equivalence classes formed by ρ on S are ρ-classes, and the ρ-class containing an element x of S will be denoted by x_ρ.

Definition 2.5. The equivalence relation ρ on a set S defined by $(x,y) \varepsilon \rho$ iff $x = y$ for each $x,y \varepsilon S$ is the equality relation on S and will be denoted by ε_S.

Definition 2.6. The equivalence relation ρ on a set S defined by $(x,y)\varepsilon\ \rho$ for each $x,y\varepsilon S$ is the universal relation on S and will be denoted by w_S. Notice that $w_S = S \times S$.

Definition 2.7. An equivalence relation ρ on a set S is proper iff $\rho \neq \varepsilon_S$.

Definition 2.8. A relation ρ on a set S is a partial ordering of S iff ρ is reflexive, antisymmetric, and transitive.

Notation. A partial ordering for a set S will normally be denoted by $\leq$; $(x,y)\varepsilon\leq$ will be denoted by $x\leq y$; $(S,\leq)$, or simply S, will be called a partially ordered set.

Definition 2.9. If $(S,\leq)$ is a partially ordered set and $B \subseteq S$, then $p\varepsilon S$ is an upper bound of B iff $b\leq p$ for each $b\varepsilon B$. Similarly, p is a lower bound of B iff $p\leq b$ for each $b\varepsilon B$.

Definition 2.10. If $(S,\leq)$ is a partially ordered set and $B \subseteq S$, then $p\varepsilon S$ is a least upper bound of B iff (i) p is an upper bound of B, and (ii) if $q\varepsilon S$ is an upper bound of B, then $p\leq q$. Similarly, p is a greatest lower bound of B iff (i) p is a lower bound of B, and (ii) if q is a lower bound of B, then $q\leq p$.

Notation. The least upper bound and greatest lower bound of a subset B of a partially ordered set $(S,\leq)$ will be denoted by lub B and glb B, respectively.

Definition 2.11. A partially ordered set $(S,\leq)$ is a lower semilattice iff for each $x,y\varepsilon S$ there exists $q\varepsilon S$ such that

$q = \text{glb}\{x,y\}$. $(S,\leq)$ is an upper semilattice iff for each $x,y \in S$ there exists $p \in S$ such that $p = \text{lub}\{x,y\}$.

Definition 2.12. A partial ordering $\leq$ on a set S is a linear ordering on S iff either $x \leq y$ or $y \leq x$ for each $x,y \in S$. In such a case, $(S,\leq)$ is called a linearly ordered set, or simply a chain.

Definition 2.13. If $(S,\leq)$ is a partially ordered set and $p \in S$, then: (i) p is the least element of S iff $p \leq x$ for each $x \in S$, (ii) p is the greatest element of S iff $x \leq p$ for each $x \in S$, (iii) p is a minimal element of S iff $x \leq p$ implies $x = p$ for each $x \in S$, and (iv) p is a maximal element of S iff $p \leq x$ implies $x = p$ for each $x \in S$.

Notation. If S is a semigroup then E_S will denote the set of all idempotent elements of S together with the binary relation $\leq$ defined by $e \leq f$ iff $e = ef = fe$.

Lemma 2.14. If S is a semigroup, then E_S is a partially ordered set.

Proof. If $e \in E_S$, then $e = ee = ee$ so that $e \leq e$ and $(E_S,\leq)$ is reflexive. If $e,f \in E_S$ such that $e \leq f$ and $f \leq e$, then $e = ef = fe$ and $f = fe = ef$ so that $e = ef = f$ and $(E_S,\leq)$ is antisymmetric. If $e,f,g \in E_S$ such that $e \leq f$ and $f \leq g$, then $e = ef = fe$ and $f = fg = gf$ so that $e = ef = e(fg) = (ef)g = eg$ and $e = fe = (gf)e = g(fe) = ge$. Therefore $e = eg = ge$ so that $e \leq g$ and $(E_S,\leq)$ is transitive.

The following proposition will give some insight into the relationship between the concepts of lower (and upper) semilattice (a partially ordered set) and a semilattice (a commutative, idempotent semigroup).

Proposition 2.15. If S is a semilattice, then $E_S = S$ is a lower semilattice with $glb\{x,y\} = xy$. Conversely, if T is a lower semilattice, then $(T,*)$ is a semilattice, where $x*y = glb\{x,y\}$ for all $x,y \varepsilon T$.

Proof. If S is a semilattice then $E_S = S$. Therefore, if $x,y \varepsilon E_S$ then $xy = xxy$ (since S is idempotent) $= xyx$ (since S is commutative), and so $xy \leq x$. Similarly, $xy = xyy = yxy$ so that $xy \leq y$ and thus xy is a lower bound for $\{x,y\}$. Now if p is a lower bound for $\{x,y\}$ then $p \leq x$ and $p \leq y$ so that $p = px = xp$ and $p = py = yp$. Therefore $p = pp = (px)(py) = (pp)(xy) = p(xy) = (xy)p$, so that $p \leq xy$ and $xy = glb\{x,y\}$. Conversely, if T is a lower semilattice, then define the multiplication $*$ on T by $x*y = glb\{x,y\}$ for all $x,y \varepsilon T$. If $x,y \varepsilon T$, then since T is a semilattice, there exists $p \varepsilon T$ such that $p = glb\{x,y\} = x*y$. Therefore $x*y \varepsilon T$ and so $*$ is a binary relation on T. If $x,y,z \varepsilon T$ then $(x*y)*z = glb\{glb\{x,y\},z\}$ so that $(x*y)*z \leq glb\{x,y\}$ and $(x*y)*z \leq z$. Therefore $(x*y)*z \leq x$, $(x*y)*z \leq y$, and $(x*y)*z \leq z$, so that $(x*y)*z$ is a lower bound for $\{x,y,z\}$. Now if p is a lower bound for $\{x,y,z\}$, then p is a lower bound for $\{x,y\}$ and for $\{z\}$, so that $p \leq glb\{x,y\}$ and $p \leq z$. Therefore p is a lower bound for $\{glb\{x,y\},z\}$, and so $p \leq glb\{glb\{x,y\},z\} = (x*y)*z$. Thus $(x*y)*z = glb\{x,y,z\}$. Similarly, $x*(y*z) = glb\{x,y,z\}$, so that $(x*y)*z = x*(y*z)$ and T is associative under $*$. Since T is a lower semilattice, then T is partially ordered, so that $x \leq x$ for each $x \in T$ and thus x is a lower bound for $\{x,x\}$. Also, if b is a lower bound for $\{x,x\}$, then $b \leq x$, so that $x = \text{glb}\{x,x\} = x*x$ and $(T,*)$ is idempotent. Finally, if $x,y \in T$, then $x*y = \text{glb}\{x,y\} = \text{glb}\{y,x\} = y*x$, and so $(T,*)$ is commutative. Thus $(T,*)$ is a semilattice.

Definition 2.16. An equivalence relation ρ on a semigroup S is a left congruence on S iff $(a,b) \in \rho$ implies $(ca,cb) \in \rho$ for all $a,b,c \in S$; ρ is a right congruence on S iff $(a,b) \in \rho$ implies $(ac,bc) \in \rho$ for all $a,b,c \in S$; ρ is a congruence on S iff ρ is both a left and a right congruence on S. A (left or right) congruence ρ on a semigroup S is proper iff ρ is proper as an equivalence relation.

Lemma 2.17. An equivalence relation ρ on a semigroup S is a congruence iff $(w,x) \in \rho$ and $(y,z) \in \rho$ imply $(wy,xz) \in \rho$.

Proof. If ρ is a congruence on S and $w,x,y,z \in S$ such that $(w,x) \in \rho$ and $(y,z) \in \rho$, then $(wy,xy) \in \rho$ since ρ is a right congruence and $(xy,xz) \in \rho$ since ρ is a left congruence. Therefore $(wy,xz) \in \rho$ since ρ is transitive. Conversely, if $(w,x) \in \rho$ and $(y,z) \in \rho$ imply $(wy,xz) \in \rho$, then let $(a,b) \in \rho$. For each $c \in S$, $(c,c) \in \rho$ since ρ is reflexive. Therefore $(ca,cb) \in \rho$ and $(ac,bc) \in \rho$, and so ρ is a congruence on S.

This lemma leads to the following concept of a quotient semigroup.

Definition 2.18. Let ρ be a congruence on a semigroup S, and let S/ρ be the collection of disjoint ρ-classes. Let * be the binary relation on S/ρ defined by $(x_\rho)*(y_\rho) = (xy)_\rho$ for all $x_\rho, y_\rho \in S/\rho$. Then $(S/\rho, *)$ is the quotient semigroup of S relative to the congruence ρ.

Observe that if $x_\rho, y_\rho \in S/\rho$ then $(x_\rho)(y_\rho) = (xy)_\rho \in S/\rho$ since $xy \in S$, so that multiplication in S/ρ is closed. Furthermore, if $x_\rho, y_\rho, z_\rho \in S/\rho$, then $[(x_\rho)(y_\rho)](z_\rho) = (xy)_\rho(z_\rho) = [(xy)z]_\rho = [x(yz)]_\rho = (x_\rho)(yz)_\rho = (x_\rho)[(y_\rho)(z_\rho)]$, so that multiplication in S/ρ is associative. Thus S/ρ with the operation defined above is indeed a semigroup. In fact, the concept of quotient semigroup with respect to a congruence is a generalization of the notion of quotient group with respect to a normal subgroup. The following theorem expresses this fact.

Theorem 2.19. If N is a normal subgroup of a group G, then there exists a congruence ρ on G such that $G/\rho = G/N$. Conversely, if ρ is a congruence on a group G, then there exists a normal subgroup N of G such that $G/N = G/\rho$.

Proof. If N is a normal subgroup of G, then define the relation ρ on G by $(x,y) \in \rho$ iff $xN = yN$ for all $x,y \in G$. Since $xN = xN$ for each $x \in G$, then $(x,x) \in \rho$ and so ρ is reflexive. If $(x,y) \in \rho$, then $xN = yN$. Therefore $yN = xN$, so that $(y,x) \in \rho$ and ρ is symmetric. If $(x,y),(y,z) \in \rho$ then $xN = yN$ and $yN = zN$, so that $xN = zN$, $(x,z) \in \rho$, and ρ is transitive. Furthermore, if $(w,x) \in \rho$ and $(y,z) \in \rho$, then $wN = xN$ and $yN = zN$. Therefore $(wy)N = (wN)(yN) = (xN)(zN) = (xz)N$, so that $(wy,xz) \in \rho$ and ρ is a congruence on G. Thus G/ρ is the quotient semigroup whose elements are the disjoint ρ-classes. To verify that $G/\rho = G/N$, notice that the definition of ρ states that if $x,y \in G$, then x and y are in the same ρ-class iff x and y are in the same left coset of N. Indeed, if $a \in G$, then $a_\rho = \{x \in G \mid (x,a) \in \rho\} = \{x \in G \mid xN = aN\} = aN$, so that the ρ-classes and left cosets of N coincide. Therefore, if $a,b \in G$, then $a_\rho = aN$, $b_\rho = bN$, and $(ab)_\rho = (ab)N$, so that $(a_\rho)(b_\rho) = (ab)_\rho = (ab)N = (aN)(bN)$. Thus each ρ-class corresponds to an identical (set-wise) left coset, each left coset corresponds to an identical ρ-class, and the product of two ρ-classes is the same as the product of the corresponding left cosets, so that $G/\rho = G/N$. Conversely, if ρ is a congruence on a group G, then ρ partitions G into disjoint ρ-classes. Therefore, if 1 is the identity for G, then $1_\rho \neq \phi$ since $1 \in 1_\rho$. Also, if $x,y \in 1_\rho$, then $(x,1) \in \rho$ and $(y,1) \in \rho$, so that $(1,y) \in \rho$ by symmetry. Thus $(x,y) = (x\cdot 1, 1\cdot y) = (x,1)(1,y) \in \rho$. However, since $(y^{-1}, y^{-1}) \in \rho$, then $(xy^{-1},1) = (xy^{-1},yy^{-1}) = (x,y)(y^{-1},y^{-1}) \in \rho$. Therefore $xy^{-1} \in 1_\rho$ and so 1_ρ is a subgroup of G. Now if $x \in G$ and $a \in 1_\rho$, then $a_\rho = 1_\rho$. Therefore $(xax^{-1})_\rho = x_\rho a_\rho x_\rho^{-1} = x_\rho 1_\rho x_\rho^{-1} = (x1x^{-1})_\rho = 1_\rho$, so that $xax^{-1} \in 1_\rho$ and 1_ρ is normal in G. For each $a \in G$, if $x \in a1_\rho$, then there exists $y \in 1_\rho$ such that $x = ay$. Therefore $x_\rho = (ay)_\rho = a_\rho y_\rho = a_\rho 1_\rho = (a1)_\rho = a_\rho$, so that $x \in a_\rho$ and $a1_\rho \subseteq a_\rho$. For each $x \in a_\rho$, $x_\rho = a_\rho = (a1)_\rho = a_\rho 1_\rho$, so that $(a^{-1}x)_\rho = a_\rho^{-1} x_\rho = a_\rho^{-1}(a_\rho 1_\rho) = (a_\rho^{-1} a_\rho) 1_\rho = (a^{-1}a)_\rho 1_\rho = 1_\rho 1_\rho = 1_\rho$. Therefore $a^{-1}x \in 1_\rho$, so that $x \in a1_\rho$ and $a_\rho \subseteq a1_\rho$.

Thus $a1_\rho = a_\rho$, and the left cosets of 1_ρ coincide with the ρ-classes. Furthermore, for each $a,b \in G$, since $(ab)1_\rho = (ab)_\rho$, then $(a1_\rho)(b1_\rho) = (ab)1_\rho = (ab)_\rho = (a_\rho)(b_\rho)$, so that the product of cosets in $G/1_\rho$ is identical (set-wise) to the product of the corresponding ρ-classes in G/ρ, and so $G/1_\rho = G/\rho$.

Before the next notion is introduced, it should be pointed out that the intersection of any collection of congruences on a semigroup S is also a congruence on S. This fact is stated in the following lemma.

<u>Lemma 2.20</u>. If $\{\rho_\alpha\}_{\alpha \in A}$ is a collection of congruences on a semigroup S, then $\bigcap_{\alpha \in A} \rho_\alpha$ is a congruence on S.

<u>Proof</u>. If $x \in S$ then $(x,x) \in \rho_\alpha$ for each $\alpha \in A$, so that $(x,x) \in \bigcap_{\alpha \in A} \rho_\alpha$ and $\bigcap_{\alpha \in A} \rho_\alpha$ is reflexive. If $(x,y) \in \bigcap_{\alpha \in A} \rho_\alpha$, then $(x,y) \in \rho_\alpha$ for each $\alpha \in A$. Therefore $(y,x) \in \rho_\alpha$ for each $\alpha \in A$, so that $(y,x) \in \bigcap_{\alpha \in A} \rho_\alpha$ and $\bigcap_{\alpha \in A} \rho_\alpha$ is symmetric. If (x,y), $(y,z) \in \bigcap_{\alpha \in A} \rho_\alpha$, then $(x,y) \in \rho_\alpha$ and $(y,z) \in \rho_\alpha$ for each $\alpha \in A$. Therefore $(x,z) \in \rho_\alpha$ for each $\alpha \in A$, so that $(x,z) \in \bigcap_{\alpha \in A} \rho_\alpha$, and $\bigcap_{\alpha \in A} \rho_\alpha$ is transitive. Finally, if (w,x), $(y,z) \in \bigcap_{\alpha \in A} \rho_\alpha$, then $(w,x) \in \rho_\alpha$ and $(y,z) \in \rho_\alpha$ for each $\alpha \in A$. Therefore $(wy,xz) \in \rho_\alpha$ for each $\alpha \in A$, so that $(wy,xz) \in \bigcap_{\alpha \in A} \rho_\alpha$ and $\bigcap_{\alpha \in A} \rho_\alpha$ is a congruence on S.

<u>Definition 2.21</u>. If ρ is a binary relation on a semigroup S, then the congruence on S generated by ρ is the intersection of all congruences on S containing ρ.

<u>Definition 2.22</u>. If S and T are semigroups, then a function f mapping S into T is a homomorphism of S into T iff $f(x) \cdot f(y) = f(xy)$ for each $x,y \in S$. A function $f: S \to T$ is an

embedding of S into T iff f is a one-to-one homomorphism, and S is said to be embeddable in T. The semigroup T is a homomorphic image of S iff there exists a homomorphism of S onto T. A function $f:S \to T$ is an isomorphism of S onto T iff f is a one-to-one onto homomorphism, in which case S and T are said to be isomorphic, written $S \cong T$. A function $f:S \to S$ is an endomorphism iff f is a homomorphism, and $f:S \to S$ is an automorphism iff f is an isomorphism.

Notation: If f is a function from a set A into a set B, then the domain A of f will be denoted by D_f, and the range B of f will be denoted by R_f.

Lemma 2.23 (Fundamental Theorem of Semigroup Homomorphisms). If f is a homomorphism of a semigroup S into a semigroup T, then the relation ρ on S defined by $(a,b) \in \rho$ iff $f(a) = f(b)$ for all $a,b \in S$ is a congruence on S and $S/\rho \cong f(S)$. Conversely, if ρ is a congruence on a semigroup S, then the function $f:S \to S/\rho$ defined by $f(a) = a_\rho$ for each $a \in S$ is a homomorphism of S onto S/ρ.

Proof. Let f be a homomorphism from a semigroup S into a semigroup T. Define the relation ρ on S by $(a,b) \in \rho$ iff $f(a) = f(b)$ for all $a,b \in S$. Since $f(x) = f(x)$ for each $x \in S$, then $(x,x) \in \rho$ and ρ is reflexive. If $(x,y) \in \rho$ then $f(x) = f(y)$, so that $f(y) = f(x)$. Therefore $(y,x) \in \rho$ and ρ is symmetric. If $(x,y), (y,z) \in \rho$ then $f(x) = f(y)$ and $f(y) = f(z)$, so that $f(x) = f(z)$, $(x,z) \in \rho$, and ρ is transitive. If $(w,x), (y,z) \in \rho$ then $f(w) = f(x)$ and $f(y) = f(z)$, so that

$f(wy) = f(w)\cdot f(y) = f(x)\cdot f(z) = f(xz)$, and thus ρ is a congruence on S by lemma 2.17. Now define $g: S/\rho \to f(S)$ by $g(a_\rho) = f(a)$ for all $a_\rho \in S/\rho$. If $(x,y) \in g$ then $x \in S/\rho$, and so there exists $a \in S$ such that $x = a_\rho$. Therefore $y = g(x) = g(a_\rho) = f(a) \in f(S)$, and so $g \subseteq S/\rho \times f(S)$. If $a,b \in S$ such that $a_\rho = b_\rho$, then $(a,b) \in \rho$, so that $f(a) = f(b)$. Thus $g(a_\rho) = g(b_\rho)$, and so g is a well-defined function. If $a,b \in S$ such that $g(a_\rho) = g(b_\rho)$, then $f(a) = f(b)$. Therefore $(a,b) \in \rho$, so that $a_\rho = b_\rho$ and g is one-to-one. If $x \in f(S)$ then there exists $a \in S$ such that $x = f(a)$. Since $a \in S$, then $a_\rho \in S/\rho$, so that $g(a_\rho) = f(a) = x$, and so g is onto. Finally, if $a_\rho, b_\rho \in S/\rho$, then $g(a_\rho b_\rho) = g[(ab)_\rho] = f(ab) = f(a)\cdot f(b) = g(a_\rho)\cdot g(b_\rho)$, so that g is a homomorphism. Thus $g: S/\rho \to f(S)$ is an isomorphism and $S/\rho \cong f(S)$.

Conversely, if ρ is a congruence on a semigroup S, then define $f: S \to S/\rho$ by $f(a) = a_\rho$ for all $a \in S$. If $(x,y) \in f$, then $x \in S$, so that $y = f(x) = x_\rho \in S/\rho$ and $f \subseteq S \times S/\rho$. If $a,b \in S$ such that $a = b$, then $(a,b) \in \rho$ since ρ is reflexive. Therefore $a_\rho = b_\rho$, so that $f(a) = f(b)$, and thus f is a well-defined function. If $y \in S/\rho$, then there exists $x \in S$ such that $y = x_\rho$. Since $x \in S$, then $f(x) = x_\rho = y$, and so f is onto. Finally, if $a,b \in S$, then $f(ab) = (ab)_\rho = (a_\rho)\cdot(b_\rho) = f(a)\cdot f(b)$, so that f is a homomorphism.

<u>Definition 2.24</u>. If f is a homomorphism of a semigroup S into a semigroup T, then the congruence ρ on S defined by

$(a,b) \in \rho$ iff $f(a) = f(b)$ for all $a,b \in S$ is called the congruence on S induced by f.

Definition 2.25. If ρ is a congruence on a semigroup S, then the homomorphism $f:S \to S/\rho$ of S onto S/ρ defined by $f(a) = a_\rho$ for all $a \in S$ is called the natural homomorphism of S onto S/ρ.

Lemma 2.26. Let ρ be a congruence on a semigroup S. For each congruence α on S containing ρ, define a binary relation α' on S/ρ by $(x_\rho, y_\rho) \in \alpha'$ iff $(x,y) \in \alpha$ for all $x,y \in S$. Then the mapping f defined by $f(\alpha) = \alpha'$ is a one-to-one, order preserving mapping of the set of all congruences on S containing ρ onto the set of all congruences on S/ρ.

Proof. Let ρ be a congruence on a semigroup S. Define $A = \{\alpha | \alpha$ is a congruence on S and $\rho \subseteq \alpha\}$. For each $\alpha \in A$, define α' on S/ρ by $(x_\rho, y_\rho) \in \alpha'$ iff $(x,y) \in \alpha$. Define $B = \{\alpha' | \alpha \in A\}$, and define the mapping $f:A \to B$ by $f(\alpha) = \alpha'$ for all $\alpha \in A$. Define $P = \{\delta | \delta$ is a congruence on $S/\rho\}$. The first objective will be to show that the set B of all images of elements of A under f is actually the same as P.

Part I: If $\alpha' \in B$ then there exists $\alpha \in A$ such that $\alpha' = f(\alpha)$. Now if $x_\rho \in S/\rho$ then $x \in S$, so that $(x,x) \in \alpha$. Therefore $(x_\rho, x_\rho) \in \alpha'$ and so α' is reflexive. If $x_\rho, y_\rho \in S/\rho$ such that $(x_\rho, y_\rho) \in \alpha'$, then $(x,y) \in \alpha$. Thus $(y,x) \in \alpha$, so that $(y_\rho, x_\rho) \in \alpha'$ and α' is symmetric. If $x_\rho, y_\rho, z_\rho \in S/\rho$ such that $(x_\rho, y_\rho) \in \alpha'$ and $(y_\rho, z_\rho) \in \alpha'$, then $(x,y) \in \alpha$ and $(y,z) \in \alpha$. Therefore $(x,z) \in \alpha$, so that $(x_\rho, z_\rho) \in \alpha'$ and α' is transitive. Finally, if $w_\rho, x_\rho, y_\rho, z_\rho \in S/\rho$ such that

$(w_\rho, x_\rho) \varepsilon \alpha'$ and $(y_\rho, z_\rho) \varepsilon \alpha'$, then $(w,x) \varepsilon \alpha$ and $(y,z) \varepsilon \alpha$. Therefore $(wy,xz) \varepsilon \alpha$, so that

$$(w_\rho y_\rho, x_\rho z_\rho) = ((wy)_\rho, (xz)_\rho) \varepsilon \alpha'.$$

Thus α' is a congruence on S/ρ, so that $\alpha' \varepsilon P$ and $B \subseteq P$. Conversely, if $\delta \varepsilon P$, then δ is a congruence on S/ρ. Define λ on S by $(x,y) \varepsilon \lambda$ iff $(x_\rho, y_\rho) \varepsilon \delta$ for all $x,y \varepsilon S$. If $x \varepsilon S$ then $x_\rho \varepsilon S/\rho$. Therefore $(x_\rho, x_\rho) \varepsilon \delta$, so that $(x,x) \varepsilon \lambda$ and λ is reflexive. If $(x,y) \varepsilon \lambda$ then $(x_\rho, y_\rho) \varepsilon \delta$. Thus $(y_\rho, x_\rho) \varepsilon \delta$, so that $(y,x) \varepsilon \lambda$ and λ is symmetric. If $(x,y), (y,z) \varepsilon \lambda$, then $(x_\rho, y_\rho) \varepsilon \delta$ and $(y_\rho, z_\rho) \varepsilon \delta$. Therefore $(x_\rho, z_\rho) \varepsilon \delta$, so that $(x,z) \varepsilon \lambda$ and λ is transitive. Furthermore, if $(w,x), (y,z) \varepsilon \lambda$, then $(w_\rho, x_\rho) \varepsilon \delta$ and $(y_\rho, z_\rho) \varepsilon \delta$. Therefore $((wy)_\rho, (xz)_\rho) = (w_\rho y_\rho, x_\rho z_\rho) \varepsilon \delta$, so that $(wy, xz) \varepsilon \lambda$ and λ is a congruence on S. Finally, if $x,y \varepsilon S$ such that $(x,y) \varepsilon \rho$, then $x_\rho = y_\rho$. Thus $(x_\rho, y_\rho) = (x_\rho, x_\rho) \varepsilon \delta$, so that $(x,y) \varepsilon \lambda$ and $\rho \subseteq \lambda$. Therefore λ is a congruence on S containing ρ, and so there exists $\alpha \varepsilon A$ such that $\lambda = \alpha$. Since $(x_\rho, y_\rho) \varepsilon \delta$ iff $(x,y) \varepsilon \lambda = \alpha$, then $\delta = \alpha' \varepsilon B$, so that $P \subseteq B$. This concludes that $B = P = \{\delta | \delta$ is a congruence on $S/\rho\}$.

Part II: Now if $(x,y) \varepsilon f$, then $x \varepsilon A$. Therefore $f(x) = x' \varepsilon B$, so that $f \subseteq A \times B$. If $\alpha_1, \alpha_2 \varepsilon A$ such that $\alpha_1 = \alpha_2$, then $(a_\rho, b_\rho) \varepsilon \alpha_1'$ iff $(a,b) \varepsilon \alpha_1 = \alpha_2$ iff $(a_\rho, b_\rho) \varepsilon \alpha_2'$. Therefore $\alpha_1' = \alpha_2'$, so that $f(\alpha_1) = f(\alpha_2)$ and f is a well-defined function. If $\alpha_1, \alpha_2 \varepsilon A$ such that $f(\alpha_1) = f(\alpha_2)$, then $\alpha_1' = \alpha_2'$. Thus $(a,b) \varepsilon \alpha_1$ iff $(a_\rho, b_\rho) \varepsilon \alpha_1' = \alpha_2'$ iff $(a,b) \varepsilon \alpha_2$, so that $\alpha_1 = \alpha_2$ and f is one-to-one. If $\alpha' \varepsilon B$, then by definition of B there exists $\alpha \varepsilon A$ such that $f(\alpha) = \alpha'$, so that f is onto. Finally, suppose $\alpha_1, \alpha_2 \varepsilon A$ such that $\alpha_1 \subseteq \alpha_2$. If $(a_\rho, b_\rho) \varepsilon f(\alpha_1) = \alpha_1'$, then $(a,b) \varepsilon \alpha_1 \subseteq \alpha_2$, so that $(a_\rho, b_\rho) \varepsilon \alpha_2' = f(\alpha_2)$ and f preserves the order of A and B relative to set containment.

Definition 2.27. If A is a set, then the function i_A on A defined by $i_A(x) = x$ for all $x \varepsilon A$ is the identity function on A.

Definition 2.28. If f is a function and $\phi \neq A \subseteq D_f$, then $f|A = \{(x,y) \varepsilon f | x \varepsilon A\}$. Thus $f|A$ is a function from the subset A of D_f into R_f so that $f|A(x) = f(x)$ for each $x \varepsilon D_{f|A} = A \subseteq D_f$.

Definition 2.29. If A is a set, then 2^A, called the power set of A, will denote the collection of all subsets of A.

Definition 2.30. A transformation on a set A is a function $f: A \rightarrow A$ from A into A.

CHAPTER BIBLIOGRAPHY

1. Petrich, Mario, *Introduction to Semigroups*, Columbus, Ohio, Charles E. Merrill Publishing Company, 1973.

2. Shapiro, Louis, *Introduction to Abstract Algebra*, New York, McGraw-Hill Book Company, Inc., 1975.

CHAPTER III

SUMMARY OF GENERAL PROPERTIES, EXAMPLES, AND THE EMBEDDING THEOREM

Example 3.1. The set $\tau(A)$ of all transformations on a nonempty set A under the operation $\circ$ of composition of functions is a semigroup.

Proof. If A is nonempty, then the identity mapping $i_A: A \to A$ is an element of $\tau(A)$, and so $\tau(A)$ is nonempty. Furthermore, if $f,g,h \in \tau(A)$, then $f: A \to A$ and $g: A \to A$. Therefore $f \circ g: A \to A$, so that $f \circ g \in \tau(A)$. Finally, for each $x \in A$, $[f \circ (g \circ h)](x) = f[(g \circ h)(x)] = f[g(h(x))] = (f \circ g)[h(x)] = [(f \circ g) \circ h](x)$, so that $f \circ (g \circ h) = (f \circ g) \circ h$. Therefore $\tau(A)$ is associative under composition of functions and is thus a semigroup.

Example 3.2. Under the operation $\circ$ of composition of functions, the collection K(A) of all constant transformations in $\tau(A)$ is a left zero subsemigroup of $\tau(A)$, where $A \neq \phi$.

Proof. Since $A \neq \phi$, then there exists $p \in A$. Therefore the function $f: A \to A$ defined by $f(x) = p$ for all $x \in A$ is an element of K(A), so that $K(A) \neq \phi$. Furthermore, if $f,g \in K(A)$, then there exists $p,q \in A$ such that $f(x) = p$ and $g(x) = q$ for all $x \in A$. Therefore, $f \circ g(x) = f[g(x)] = f(q) = p = f(x)$ for all $x \in A$, so that $f \circ g = f \in K(a)$. Associativity in K(A) is inherited from $\tau(A)$. Since it is obvious that $K(A) \subseteq \tau(A)$, then $K(A)$ is a subsemigroup of $\tau(A)$. However, since it has already been shown that $f \circ g = f$ for each $f, g \in K(A)$, then $K(A)$ is a left zero subsemigroup of $\tau(A)$.

Example 3.3. If $A \neq \phi$, then $K(A)$ is an ideal of $\tau(A)$.

Proof. If $f \in K(A)$ and $g \in \tau(A)$, then there exists $p \in A$ such that $f(x) = p$ for all $x \in A$. However, since $p \in A$, then there exists $q \in A$ such that $g(p) = q$. Therefore, for all $x \in A$, $(f \circ g)(x) = f[g(x)] = p$ since $g(x) \in A$, and so $f \circ g \in K(A)$. Also, for all $x \in A$, $(g \circ f)(x) = g[f(x)] = g(p) = q$, and so $g \circ f \in K(A)$. Thus $K(A)$ is an ideal in $\tau(A)$.

Lemma 3.4. Let $M, N \in Z^+$, and let A be a set such that $|A| = N$; then $B = \{f \in \tau(A) \mid |f(A)| \leq M\}$ is an ideal of $\tau(A)$.

Proof. If $f \in B$ and $g \in \tau(A)$, then there exists $M \leq N$, such that $|f(A)| = M$. Therefore, there exists $\{a_i\}_{i=1}^{M} \subseteq A$ such that for all $x \in A$, $f(x) \in \{a_i\}_{i=1}^{M}$. If $x \in A$, then $(f \circ g)(x) = f[g(x)] \in \{a_i\}_{i=1}^{M}$ since $g(x) \in A$. Therefore $|(f \circ g)(A)| \leq M \leq N$, so that $f \circ g \in B$. Furthermore, if $x \in A$, then $(g \circ f)(x) = g[f(x)] = g(a_i)$ for some i, $i \leq i \leq M$. Therefore, $(g \circ f)(x) \in \{g(a_i)\}_{i=1}^{M}$ for all $x \in A$, so that $|(g \circ f)(A)| \leq M \leq N$ and $g \circ f \in B$. Finally, since $|A| = N > 0$, then there exists $p \in A$. Therefore, the function $f: A \to A$ defined by $f(x) = p$ for all $x \in A$ is an element of B, since $|f(A)| = 1$ and $N \in Z^+$ imply $|f(A)| \leq N$. Thus $B \neq \phi$, and so B is an ideal of $\tau(A)$.

Theorem 3.5. If $\tau(A)$ is the semigroup of transformations on a nonempty set A and $\alpha \varepsilon \tau(A)$, then $\alpha\tau(A) = \tau(A)$ iff $\tau(A)\alpha = \tau(A)$ iff $\alpha:A \to A$ is onto.

Proof. If $\alpha \varepsilon \tau(A)$ such that $\alpha:A \to A$ is onto and $\beta \varepsilon \tau(A)$, then for each $y \varepsilon \beta(A)$ there exists a unique $x_y \varepsilon A$ such that $\alpha(x_y) = y$. Let $\Gamma \varepsilon \tau(A)$ such that $\Gamma(x) = x_{\beta(x)}$ for each $x \varepsilon A$. Therefore, for all $x \varepsilon A$, $\alpha \circ \Gamma(x) = \alpha[\Gamma(x)] = \alpha[x_{\beta(x)}] = \beta(x)$, so that $\beta = \alpha \circ \Gamma \varepsilon \alpha\tau(A)$ and $\tau(A) \subseteq \alpha\tau(A)$. Since $\alpha\tau(A) \subseteq \tau(A)$ as well, then $\alpha\tau(A) = \tau(A)$.

If $\alpha \varepsilon \tau(A)$ such that $\alpha\tau(A) = \tau(A)$, then there exists $\Gamma \varepsilon \tau(A)$ such that $\alpha \circ \Gamma = i_A$. Therefore, for each $y \varepsilon A$ there exists $\Gamma(y) \varepsilon A$ such that $\alpha[\Gamma(y)] = \alpha \circ \Gamma(y) = i_A(y) = y$, and so $\alpha:A \to A$ is onto.

If $\alpha \varepsilon \tau(A)$ such that $\alpha:A \to A$ is onto and $\beta \varepsilon \tau(A)$, then for each $y \varepsilon A$ there exists a unique $x_y \varepsilon A$ such that $\alpha(x_y) = y$, so that $x_y = \alpha^{-1}(y)$. Let $\Gamma \varepsilon \tau(A)$ such that $\Gamma(y) = \beta[\alpha^{-1}(y)]$ for each $y \varepsilon A$. Notice that since $\alpha:A \to A$ is onto, then α is one-to-one, so that $\alpha^{-1}(y)$ is unique and Γ is indeed a function on A. Therefore, for all $x \varepsilon A$, $\Gamma \circ \alpha(x) = \Gamma[\alpha(x)] = \beta(\alpha^{-1}[\alpha(x)]) = \beta(x)$, so that $\beta = \Gamma \circ \alpha \varepsilon \tau(A)\alpha$. Thus $\tau(A) \subseteq \tau(A)\alpha$, and so $\tau(A)\alpha = \tau(A)$.

Finally, if $\alpha \varepsilon \tau(A)$ such that $\tau(A)\alpha = \tau(A)$, then there exists $\Gamma \varepsilon \tau(A)$ such that $\Gamma \circ \alpha = i_A$, which is one-to-one. Therefore Γ is one-to-one as well. Now if $y \varepsilon A$, then $x = \Gamma(y) \varepsilon A$. Thus $\Gamma[\alpha(x)] = \Gamma \circ \alpha(x) = i_A(x) = x = \Gamma(y)$, so that $\alpha(x) = y$ and $\alpha:A \to A$ is onto.

Theorem 3.6. If A is a nonempty set, then:

(1) $E_{\tau(A)} = \{\alpha \in \tau(A) | x \in \alpha^{-1}(x) \text{ or } \alpha^{-1}(x) = \phi \text{ for all } x \in A\}$,

(2) if $\alpha \in E_{\tau(A)}$, then $G_{\alpha} = \{f \in \tau(A) | f \text{ is regular and } \alpha = f \circ f^{-1} = f^{-1} \circ f\}$,

(3) if $\alpha, \beta \in E_{\tau(A)}$, then $\alpha \leq \beta$ iff $\alpha(A) \subseteq \beta(A)$ and $\beta^{-1}(x) \subseteq \alpha^{-1} \circ \alpha(x)$ for all $x \in A$,

(4) if $\alpha \in \tau(A)$, then α is a left zero of $\tau(A)$ iff α is a constant function,

(5) $\tau(A)$ has no right zeros,

(6) the kernel of $\tau(A)$ is the collection of all constant functions, or left zeros, of $\tau(A)$, and

(7) $\tau(A)$ is regular.

Proof. Part I: Let $\alpha \in \tau(A)$ such that for each $x \in A$, either $x \in \alpha^{-1}(x)$ or $\alpha^{-1}(x) = \phi$. If $x \in A$, then $y = \alpha(x) \in A$, so that $x \in \alpha^{-1}(y)$. Since $\alpha^{-1}(y) \neq \phi$, then $y \in \alpha^{-1}(y)$, and so $\alpha(y) = y$. Therefore $\alpha \circ \alpha(x) = \alpha[\alpha(x)] = \alpha(y) = y = \alpha(x)$, for each $x \in A$, so that $\alpha \circ \alpha = \alpha$ and α is idempotent.

Conversely, if α is an idempotent of $\tau(A)$, then $\alpha \circ \alpha = \alpha$. If $x \in A$ such that $\alpha^{-1}(x) \neq \phi$, then there exists $y \in \alpha^{-1}(x)$, so that $\alpha(y) = x$. Therefore $\alpha(x) = \alpha[\alpha(y)] = \alpha \circ \alpha(y) = \alpha(y) = x$, and so $x \in \alpha^{-1}(x)$. Thus α is idempotent in $\tau(A)$ iff either $x \in \alpha^{-1}(x)$ or $\alpha^{-1}(x) = \phi$ for all $x \in A$, so that $E_{\tau(A)} = \{\alpha \in \tau(A) | x \in \alpha^{-1}(x) \text{ or } \alpha^{-1}(x) = \phi \text{ for all } x \in A\}$.

Part II: Furthermore, if $\alpha \in E_{\tau(A)}$, then the corresponding maximal subgroup of $\tau(A)$ is

$G_\alpha = \{f \in \tau(A) | f = \alpha \circ f = f \circ \alpha,\ \alpha = f \circ g = g \circ f$ for some $g \in \tau(A)\} = \{f \in \tau(A) | f = f \circ \alpha = f \circ (g \circ f) = f \circ g \circ f$ for some $g \in \tau(A)$, and $\alpha = f \circ g = g \circ f\}$.

However, if $f, g \in \tau(A)$ such that $f = f \circ g \circ f$, then f is regular and the inverse for f is $f^{-1} = g \circ f \circ g$ by theorem 1.35. Therefore $f \circ f^{-1} = f \circ (g \circ f \circ g) = (f \circ g) \circ (f \circ g) = \alpha \circ \alpha = \alpha$, and $f^{-1} \circ f = (g \circ f \circ g) \circ f = (g \circ f) \circ (g \circ f) = \alpha \circ \alpha = \alpha$, so that $G_\alpha = \{f \in \tau(A) | f$ is regular and $\alpha = f \circ f^{-1} = f^{-1} \circ f\}$.

Part III: By lemma 2.14, the partial order $\leq$ for $E_{\tau(A)}$ is defined by $\alpha \leq \beta$ iff $\alpha = \alpha \circ \beta = \beta \circ \alpha$ for all $\alpha, \beta \in E_{\tau(A)}$. If $\alpha = \beta \circ \alpha$, then for each $x \in A$, $\alpha(x) = \beta \circ \alpha(x) = \beta[\alpha(x)] \in \beta(A)$, so that $\alpha(A) \subseteq \beta(A)$.

Conversely, if $\alpha(A) \subseteq \beta(A)$, then $\alpha(x) \in \beta(A)$ for each $x \in A$, so that there exists $p \in A$ such that $\beta(p) = \alpha(x)$. Therefore $\beta \circ \alpha(x) = \beta[\alpha(x)] = \beta[\beta(p)] = \beta \circ \beta(p) = \beta(p) = \alpha(x)$ for each $x \in A$, so that $\beta \circ \alpha = \alpha$.

Now if $\alpha = \alpha \circ \beta$, then let $x \in A$ and let $a \in \beta^{-1}(x)$ if $\beta^{-1}(x) \neq \phi$, so that $\beta(a) = x$. Therefore $\alpha(a) = \alpha \circ \beta(a) = \alpha[\beta(a)] = \alpha(x)$, so that $a \in \alpha^{-1}[\alpha(x)]$ and thus $\beta^{-1}(x) \subseteq \alpha^{-1} \circ \alpha(x)$. Also, if $\beta^{-1}(x) = \phi$, then $\beta^{-1}(x) \subseteq \alpha^{-1} \circ \alpha(x)$.

Conversely, if $\beta^{-1}(x) \subseteq \alpha^{-1} \circ \alpha(x)$ for each $x \in A$, then $x \in \beta^{-1}[\beta(x)] \subseteq \alpha^{-1} \circ \alpha[\beta(x)]$. Therefore $\alpha(x) = \alpha \circ \alpha^{-1} \circ \alpha[\beta(x)] = \alpha[\beta(x)] = \alpha \circ \beta(x)$ for each $x \in A$, so that $\alpha = \alpha \circ \beta$. Thus for each $\alpha, \beta \in E_{\tau(A)}$, $\alpha \leq \beta$ iff $\alpha = \alpha \circ \beta = \beta \circ \alpha$ iff $\beta^{-1}(x) \subseteq \alpha^{-1} \circ \alpha(x)$ for all $x \in A$ and $\alpha(A) \subseteq \beta(A)$.

Part IV: If α is a constant function in $\tau(A)$, then there exists $k \varepsilon A$ such that $\alpha(x) = k$ for all $x \varepsilon A$. Therefore, if $\beta \varepsilon \tau(A)$ then $\beta(x) \varepsilon A$ for all $x \varepsilon A$, so that $\alpha o \beta(x) = \alpha[\beta(x)] = k = \alpha(x)$. Thus $\alpha o \beta = \alpha$ for each $\beta \varepsilon \tau(A)$, so that α is a left zero of $\tau(A)$.

Conversely, if $\alpha \varepsilon \tau(A)$ is not a constant function, then there exists $a,b,x,y \varepsilon A$ such that $a \neq b$, $x \neq y$, $\alpha(a) = x$, and $\alpha(b) = y$. If $\beta \varepsilon \tau(A)$ such that $\beta(a) = b$, then $\alpha o \beta(a) = \alpha[\beta(a)] = \alpha(b) = y \neq x = \alpha(a)$. Therefore $\alpha o \beta \neq \alpha$, so that α is not a left zero of $\tau(A)$.

Part V: If $|A| > 1$, then let $\alpha \varepsilon \tau(A)$ and let $a \varepsilon A$, so that $b = \alpha(a) \varepsilon A$. Since $|A| > 1$, then there exists $c \varepsilon A$ such that $c \neq b$. Define $\beta \varepsilon \tau(A)$ such that $\beta(x) = c$ for all $x \varepsilon A$. Therefore $\beta o \alpha(a) = \beta[\alpha(a)] = \beta(b) = c \neq b = \alpha(a)$, so that $\beta o \alpha \neq \alpha$. Thus no element $\alpha \varepsilon \tau(A)$ is a right zero of $\tau(A)$.

Part VI: Lemma 3.4 established that $\{\alpha \varepsilon \tau(A) \,|\, |\alpha(A)| \leq n$ for some $n \varepsilon Z^+\}$ is a collection of ideals in $\tau(A)$. Define $J_n = \{\alpha \varepsilon \tau(A) \,|\, |\alpha(A)| \leq n\}$ for each $n \varepsilon Z^+$. Therefore, if $K = \bigcap\{G | G$ is an ideal of $\tau(A)\}$ is the kernel of $\tau(A)$, then $K \subseteq \bigcap_{n=1}^{\infty} J_n \subseteq J_1$. Now if G is an ideal of $\tau(A)$ and $\alpha \varepsilon J_1$, then α is a constant function, and so there exists $p \varepsilon A$ such that $\alpha(x) = p$ for all $x \varepsilon A$. Therefore, if $\beta \varepsilon G$, then $\alpha o \beta \varepsilon G$ since G is an ideal. However, since $\beta(x) \varepsilon A$ for each $x \varepsilon A$, then $\alpha o \beta(x) = \alpha[\beta(x)] = p = \alpha(x)$, so that $\alpha = \alpha o \beta \varepsilon G$. Thus if $\alpha \varepsilon J_1$, then $\alpha \varepsilon G$, so that $J_1 \subseteq G$. Since $J_1 \subseteq G$ for each ideal G of $\tau(A)$, then $J_1 \subseteq \bigcap\{G | G$ is an ideal of $\tau(A)\} = K$. Therefore $K \subseteq J_1 \subseteq K$, so that $K = J_1$. Thus the kernel K of $\tau(A)$ is the collection of all constant functions, or left zeros, of $\tau(A)$.

Part VII: If $f \in \tau(A)$, then for each $y \in f(A)$, $f^{-1}(y) \neq \phi$, and so there exists $a_y \in f^{-1}(y)$. Define

$$g \in \tau(A) \text{ by } g(y) = \begin{cases} a_y \text{ if } y \in f(A) \\ y \text{ if } y \notin f(A) \text{ for each } y \in A. \end{cases}$$

Therefore, for all $x \in A$, $f \circ g \circ f(x) = f(g[f(x)]) = f(a_{f(x)})$ (since $f(x) \in f(A)$) $= f(x)$ (since $a_{f(x)} \in f^{-1}[f(x)]$), so that $f = f \circ g \circ f$. Thus f is regular for each $f \in \tau(A)$, and so $\tau(A)$ is regular.

<u>Theorem 3.7</u>. Every infinite cyclic semigroup is isomorphic to the semigroup of positive integers under addition.

<u>Proof</u>. Let S be an infinite cyclic semigroup with generator $a \in S$. Therefore, for each $x \in S$, there exists $n \in Z^+$ such that $a^n = x$. Define $f: Z^+ \to S$ by $f(n) = a^n$ for all $n \in Z^+$. If $(p,q) \in f$, then $p \in Z^+$, so that $q = f(p) = a^p \in S$ and $f \subseteq Z^+ \times S$. If $m,n \in Z^+$ such that $m = n$, then $a^m = a^n$, so that $f(m) = f(n)$ and f is well defined. If $m,n \in Z^+$ such that $f(m) = f(n)$, then $a^m = a^n$. Assuming that $m \neq n$, then either $m > n$ or $m < n$. If $m > n$, then consider $\{a^i\}_{i=1}^m \subseteq S$. Since $a \in S$ is a generator for S, then $S = \{a^i\}_{i=1}^m \cup \{a^{m+k}\}_{k=1}^\infty$. If $k = 1$, then $a^{m+k} = a^{m+1} = a^m \cdot a^1 = a^n \cdot a^1 = a^{n+1}$. Since $n \leqslant m$, then $n + 1 \leq m$, so that $a^{m+k} = a^{m+1} = a^{n+1} \in \{a^i\}_{i=1}^m$ for $k = 1$. Now assume that for $k - 1 \in Z^+$, $a^{m+k-1} \in \{a^i\}_{i=1}^m$.

Therefore, there exists $p \in Z^+$, $1 \leq p \leq m$, such that $a^{m+k-1} = a^p$. Thus $a^{m+k} = a^{m+k-1+1} = a^{m+k-1} \cdot a^1 = a^p \cdot a^1 = a^{p+1}$. Since $1 \leq p \leq m$, then $2 \leq p + 1 \leq m + 1$. If $2 \leq p + 1 \leq m$, then $a^{m+k} = a^{p+1} \in \{a^i\}_{i=1}^m$. If $p + 1 = m + 1$, then by previous results, $a^{m+k} = a^{p+1} = a^{m+1} \in \{a^i\}_{i=1}^m$. Therefore, by mathematical induction, for each $k \in Z^+$, $a^{m+k} \in \{a^i\}_{i=1}^m$, so that $\{a^{m+k}\}_{k=1}^{\infty} \subseteq \{a^i\}_{i=1}^m$. Thus $S = \{a^i\}_{i=1}^m$, and so S is finite. Similarly, if $m < n$, then S is finite. Therefore, by contradiction, if $f(m) = f(n)$, then $m = n$ for all $m,n \in Z^+$, so that f is one-to-one. If $x \in S$, then there exists $n \in Z^+$ such that $a^n = x$. Therefore $f(n) = a^n = x$, and so f is onto. Finally, if $m,n \in Z^+$, then $f(m+n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$, so that f is a homomorphism. Thus $f: Z^+ \to S$ is an isomorphism and $S \cong Z^+$.

Example 3.8. The property of cyclic is not hereditary to subsemigroups of a cyclic semigroup.

Proof. The semigroup $(Z^+,+)$ of positive integers under addition is cyclic with generator 1. Now $K = Z^+ \setminus \{1\} \subseteq Z^+$ and if $m,n \in K$, then $m > 1$ and $n > 1$. Therefore $m + n > m > 1$, so that $m + n \in Z^+ \setminus \{1\} = K$ and K is a subsemigroup of Z^+. However, K is not cyclic since 2 generates only even positive integers and no integer that exceeds 2 can generate 2.

Theorem 3.9. If S is an infinite cyclic semigroup with generator $a \in S$, and $f_k: S \to S$ is the function defined by $f_k(a^n) = a^{kn}$ for all $n \in Z^+$, then $\{f_k\}_{k \in Z^+}$ is the semigroup of endomorphisms on S and is thus a subsemigroup of $\tau(S)$.

Proof. Since S is generated by $a \in S$, then for each $x \in S$, there exists $n \in Z^+$ such that $x = a^n$. If $f:S \to S$ is a function, then there exists $k \in Z^+$ such that $f(a) = a^k$. Therefore, if f is also a homomorphism, then for each $n \in Z^+$, $f(a^n) = [f(a)]^n = [a^k]^n = a^{kn}$, so that $f = f_k$. Since f_k is an endomorphism on S for all $k \in Z^+$, then $\{f_k\}_{k \in Z^+}$ is the semigroup of all endomorphisms on S.

Theorem 3.10. Every finite semigroup is periodic.

Proof. If S is a finite semigroup and $x \in S$, then the order of x is the order of the cyclic subsemigroup of S generated by x, namely $\{x^n | n \in Z^+\}$. Therefore, since $\{x^n | n \in Z^+\} \subseteq S$, then $|\langle x \rangle| = |\{x^n | n \in Z^+\}| \leq |S|$, which is finite. Thus x is of finite order, and so S is periodic.

The following example shows that the converse of this theorem is false.

Example 3.11. Let S be the set of non-negative integers and define multiplication on S by

$$x \cdot y = \begin{cases} x \text{ if } x = y \\ 0 \text{ if } x \neq y. \end{cases}$$

Then S is periodic since $|\langle x \rangle| = 1$ for all $x \in S$, but S is not finite.

Theorem 3.12. A semigroup S is a group iff S is both left and right simple.

Proof. If S is a group with identity e and P is a left ideal in S, then $P \neq \phi$ so that there exists $a \in P$. Therefore, for all $x \in S$, $x = xe = x(a^{-1}a) = (xa^{-1})a \in P$, so that $P = S$.

Similarly, if Q is a right ideal in S, then $Q \neq \phi$ so that there exists $b \varepsilon Q$. Therefore, for all $x \varepsilon S$, $x = ex = (bb^{-1})x = b(b^{-1}x) \varepsilon Q$, so that $Q = S$. Thus S is the only left or right ideal in S, and so S is both left and right simple. Conversely, suppose S is both left simple and right simple, and let $a \varepsilon S$. If $p \varepsilon Sa$ and $q \varepsilon S$, then $p = ka$ for some $k \varepsilon S$. Therefore $qp = q(ka) = (qk)a \varepsilon Sa$ since $qk \varepsilon S$, so that Sa is a left ideal in S. Since S is left simple, then $Sa = S$. Similarly, $aS = S$ for each $a \varepsilon S$ since S is right simple. Therefore, if $a \varepsilon S = aS$, then there exists $e \varepsilon S$ such that $a = ae$. But since $e \varepsilon S = Sa$, then there exists $y \varepsilon S$ such that $e = ya$. Furthermore, since $e \varepsilon S = eS$, then there exists $z \varepsilon S$ such that $e = ez$. Therefore $ee = (ya)(ez) = [y(ae)]z = (ya)z = ez = e$, so that e is idempotent in S. By proposition 1.29, e is the identity for the subgroup G_e of S defined by $G_e = \{a \varepsilon S | a \varepsilon eS \cap Se,\ e \varepsilon aS \cap Sa\}$. Since $aS = Sa = S$ and $eS = Se = S$, then $G_e = \{a \varepsilon S | a \varepsilon S \cap S, e \varepsilon S \cap S\} = \{a \varepsilon S | a \varepsilon S,\ e \varepsilon S\} = S$, and so S is the group G_e.

However, if S is a semigroup which is left simple or right simple, but not both, then S will not be a group.

Example 3.13. Let S be a left zero semigroup such that $|S| > 1$, and let P be a left ideal in S. If $x \varepsilon S$, $y \varepsilon P$, then $x = xy \varepsilon P$, so that $S \subseteq P$. Therefore $P = S$, and so S is left simple. If there exists an identity element $e \varepsilon S$, then there also exists $k \varepsilon S$ such that $k \neq e$ since $|S| > 1$. Therefore $e \cdot k = e \neq k$ since S is a left zero semigroup, so that e is not a left identity of k. This is a contradiction since e is the identity for S. Therefore S contains no identity element and thus cannot be a group.

Example 3.14. If $(F,+,\cdot)$ is a field, then $(F,\cdot)$ is a zero simple semigroup.

Proof. If $(F,+,\ )$ is a field, then $(F,\cdot)$ is a semigroup with zero 0, the identity for +. Therefore, there exists $1 \varepsilon F$ such that $x \cdot 1 = 1 \cdot x = x$ for all $x \varepsilon F$, and if $x \varepsilon F\setminus\{0\}$, then there exists $x^{-1} \varepsilon F$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$. If J is a nonzero ideal in $(F,\cdot)$, then there exists $p \varepsilon J$ such that $p \neq 0$. Therefore there exists $p^{-1} \varepsilon F$ such that $p \cdot p^{-1} = p^{-1} \cdot p = 1$. If $x \varepsilon F$, then $x = x \cdot 1 = x \cdot (p^{-1} \cdot p) = (x \cdot p^{-1}) \cdot p \ \varepsilon J$ since $p \varepsilon J$ and J is an ideal in F, so that $F \subseteq J$. Therefore $J = F$, and so $(F,\cdot)$ is zero simple.

The next two theorems will characterize specific types of ideals in semigroups. Theorem 3.15 uses the notation S^1 for a semigroup S with adjoined identity 1 in order to generalize lemma 1.11. Theorem 3.16 characterizes all left, right, and two-sided ideals in zero semigroups and left zero semigroups.

Theorem 3.15. If A is a nonempty subset of a semigroup S, then $L_A = A \cup SA = S^1A$, $R_A = A \cup AS = AS^1$, and $J_A = A \cup SA \cup AS \cup SAS = S^1AS^1$.

Proof. Part I: If $\{G_\alpha\}_{\alpha \varepsilon \Gamma}$ is the collection of all left ideals of S containing A, then $L_A = \bigcap_{\alpha \varepsilon \Gamma} G_\alpha$. Now for each $\alpha \varepsilon \Gamma$, $A \subseteq G_\alpha$, so that $A \subseteq \bigcap_{\alpha \varepsilon \Gamma} G_\alpha = L_A$. Also, since L_A is a left ideal of S and $A \subseteq L_A$, then $xa \varepsilon L_A$ for each $x \varepsilon S$, $a \varepsilon A$. Therefore $SA \subseteq L_A$, and so $A \cup SA \subseteq L_A$.

If $p \varepsilon S^1A$ then there exists $x \varepsilon S^1$, $y \varepsilon A$ such that $p = xy$. If $x \notin S$ then $x = 1$, so that $p = xy = 1y = y \varepsilon A$. If $x \varepsilon S$, then $p = xy \varepsilon SA$. Therefore, if $p \varepsilon S^1A$, then $p \varepsilon A \cup SA$, so that $S^1A \subseteq A \cup SA$.

Now $A \neq \phi$, so that there exists $p \varepsilon A$. Therefore $p = 1p \varepsilon S^1A$, and so $S^1A \neq \phi$. Also, if $x \varepsilon S$ and $y \varepsilon S^1A$, then there exist $r \varepsilon S^1$, $t \varepsilon A$ such that $y = rt$. If $r \notin S$ then $r = 1$, so that $xy = x(rt) = x(1t) = xt \varepsilon SA \subseteq S^1A$, and if $r \varepsilon S$ then $xr \varepsilon S$, so that $xy = x(rt) = (xr)t \varepsilon SA \subseteq S^1A$. Therefore, if $x \varepsilon S$ and $y \varepsilon S^1A$, then $xy \varepsilon S^1A$. Finally, $A = \{a | a \varepsilon A\} = \{1a | a \varepsilon A\} = \{1\}A \subseteq S^1A$, so that S^1A is a left ideal of S containing A. Therefore there exists $\beta \varepsilon \Gamma$ such that $S^1A = G_\beta$, and so $L_A = \bigcap_{\alpha \varepsilon \Gamma} G_\alpha \subseteq G_\beta = S^1A$. Thus $L_A \subseteq S^1A \subseteq A \cup SA \subseteq L_A$, and so $L_A = A \cup SA = S^1A$.

Part II: Similarly, if $\{G_\alpha\}_{\alpha \varepsilon B}$ is the collection of all right ideals of S containing A, then $R_A = A \cup AS = AS^1$.

Part III: If $\{G_\alpha\}_{\alpha \varepsilon \Omega}$ is the collection of all ideals of S containing A, then $J_A = \bigcap_{\alpha \varepsilon \Omega} G_\alpha$. Now for each $\alpha \varepsilon \Omega$, $A \subseteq G_\alpha$, so that $A \subseteq \bigcap_{\alpha \varepsilon \Omega} G_\alpha = J_A$. Also, if $x \varepsilon S$ and $a \varepsilon A$, then $xa \varepsilon J_A$ and $ax \varepsilon J_A$ since J_A is an ideal of S containing A, so that $SA \subseteq J_A$ and $AS \subseteq J_A$. Furthermore, if $x \varepsilon SA \subseteq J_A$ and $y \varepsilon S$, then $xy \varepsilon J_A$ since J_A is an ideal of S. Therefore $SAS = (SA)S \subseteq J_A$, and so $A \cup SA \cup AS \cup SAS \subseteq J_A$.

If $p \in S^1AS^1$, then there exist $x,z \in S^1$, $y \in A$ such that $p = xyz$. If $x \notin S$ and $z \notin S$, then $x = 1 = z$, so that $p = xyz = 1y1 = y \in A \subseteq A \cup SA \cup AS \cup SAS$. If $x \in S$ and $z \notin S$, then $z = 1$, so that $p = xyz = xy1 = xy \in SA \subseteq A \cup SA \cup AS \cup SAS$. If $x \notin S$ and $z \in S$, then $x = 1$, so that $p = xyz = 1yz = yz \in AS \subseteq A \cup SA \cup AS \cup SAS$. If $x \in S$ and $z \in S$, then $p = xyz \in SAS \subseteq A \cup SA \cup AS \cup SAS$. Therefore if $p \in S^1AS^1$, then $p \in A \cup SA \cup AS \cup SAS$, so that $S^1AS^1 \subseteq A \cup SA \cup AS \cup SAS$.

Now $A \neq \phi$ and $A = \{1\}A\{1\} \subseteq S^1AS^1$, so that $S^1AS^1 \neq \phi$ and $A \subseteq S^1AS^1$. Furthermore, if $x \in S$ and $y \in S^1AS^1$, then there exist $p,q \in S^1$, $a \in A$ such that $y = paq$. Now $xp \in S \subseteq S^1$ whether $p \in S$ or $p = 1$, and $qx \in S \subseteq S^1$ whether $q \in S$ or $q = 1$. Therefore $xy = x(paq) = (xp)aq \in S^1AS^1$ and $yx = (paq)x = pa(qx) \in S^1AS^1$, and so S^1AS^1 is an ideal of S containing A. Hence there exists $\beta \in \Omega$ such that $S^1AS^1 = G_\beta$, so that $J_A = \bigcap_{\alpha \in \Omega} G_\alpha \subseteq G_\beta = S^1AS^1$. Thus

$$J_A \subseteq S^1AS^1 \subseteq A \cup SA \cup SA \cup SAS \subseteq J_A,$$

and so $J_A = A \cup SA \cup AS \cup SAS = S^1AS^1$.

Theorem 3.16. If S is a zero semigroup, then the left, right, and two-sided ideals of S are those subsets of S containing the zero. If S is a left zero semigroup, then S is a left simple (and thus simple), while any nonempty subset of S is a right ideal of S.

Proof. Part I: If S is a zero semigroup with zero 0, then $ab = 0$ for each $a,b \in S$. Therefore, if A and B are nonempty subsets of S, then

$$AB = \{ab | a \in A, b \in B\} = \{0 | a \in A, b \in B\} = \{0\}.$$

Thus $\{L \subseteq S | L \text{ is a left ideal of } S\} = \{L \subseteq S | SL \subseteq L \neq \phi\} = \{L \subseteq S | \{0\} \subseteq L\} = \{L \subseteq S | 0 \in L\}$, $\{R \subseteq S | R \text{ is a right ideal of } S\} = \{R \subseteq S | 0 \in R\}$ similarly, and so $\{J \subseteq S | J \text{ is an ideal of } S\} = \{L \subseteq S | 0 \in L\} \cap \{R \subseteq S | 0 \in R\} = \{J \subseteq S | 0 \in J\}$. Therefore, the left, right, and two-sided ideals of S coincide and are exactly those subsets of S containing 0.

Part II: If S is a left zero semigroup, then $ab = a$ for each $a,b \in S$. Therefore, if A and B are nonempty subsets of S, then $AB = \{ab | a \in A, b \in B\} = \{a | a \in A, b \in B\} = A$. Thus $\{L \subseteq S | L \text{ is a left ideal of } S\} = \{L \subseteq S | SL \subseteq L \neq \phi\} = \{L \subseteq S | S \subseteq L\} = \{S\}$, so that S is left simple. Furthermore, $\{R \subseteq S | R \text{ is a right ideal of } S\} = \{R \subseteq S | RS \subseteq R \neq \phi\} = \{R \subseteq S | R \subseteq R \neq \phi\} = \{R \subseteq S | R \neq \phi\}$, so that any nonempty subset of S is a right ideal of S. Therefore, $\{J \subseteq S | J \text{ is an ideal of } S\} = \{S\} \cap \{R \subseteq S | R \neq \phi\} = \{S\}$, so that S is simple.

<u>Definition 3.17</u>. A subset T of Z^+ is an interval in Z^+ iff when $x,z \in T$, $x \leq y \leq z$, and $y \in Z^+$, then $y \in T$.

<u>Theorem 3.18</u>. If Z^+ is the semigroup of positive integers with multiplication defined by $xy = \max\{x,y\}$ for each $x,y \in Z^+$, then $\{\{n \in Z^+ | n \geq k\} | k \in Z^+\}$ is the collection of all ideals in Z^+. Furthermore, the congruences on Z^+ consist of all partitions of Z^+ each of whose elements are intervals in Z^+.

<u>Proof</u>. Part I: Let $k \in Z^+$ and define $P = \{n \in Z^+ | n \geq k\}$. Now $P \subseteq Z^+$ and $P \neq \phi$ since $k \in P$. If $x \in P$ and $y \in Z^+$, then

$x \geq k$, so that $xy = \max\{x,y\} \geq x \geq k$, and $yx = \max\{y,x\} \geq x \geq k$. Therefore $xy \in P$ and $yx \in P$, so that P is an ideal of Z^+.

Conversely, if P is an ideal of Z^+, then $P \subseteq Z^+$ such that $P \neq \phi$. Since Z^+ is well-ordered, there exists $k \in P$ such that $k \leq t$ for all $t \in P$. Therefore, if $n \in Z^+$ such that $n \geq k$, then $n = \max\{n,k\} = nk \in P$ since P is an ideal, so that $\{n \in Z^+ | n \geq k\} \subseteq P$. However, since $k \leq t$ for all $t \in P$, then $n \notin P$ for all $n \in Z^+$ such that $n < k$, and so $P = \{n \in Z^+ | n \geq k\}$. Therefore, P is an ideal in Z^+ iff there exists $k \in Z^+$ such that $P = \{n \in Z^+ | n \geq k\}$, so that $\{\{n \in Z^+ | n \geq k\} | k \in Z^+\}$ is the collection of all ideals in Z^+.

Part II: Let P be a partition of Z^+, each of whose elements are intervals in Z^+. Since P is a partition of Z^+, then P identifies an equivalence relation ρ on Z^+, with the elements of P as the ρ-classes. Thus each ρ-class is an interval in Z^+. If $w,x,y,z \in Z^+$, such that $(w,x) \in \rho$ and $(y,z) \in \rho$, then $w_\rho = x_\rho$ and $y_\rho = z_\rho$. If $w_\rho = y_\rho$, then $w_\rho = x_\rho = y_\rho = z_\rho$, and so $w,x,y,z \in w_\rho$. Therefore $wy = \max\{w,y\} \in w_\rho$ and $xz = \max\{x,z\} \in w_\rho$, so that $(wy,xz) \in \rho$. However, if $w_\rho \neq y_\rho$, then $w \neq y$, so that $w < y$ or $w > y$. Without loss of generality, assume $w < y$. Since each ρ-class is an interval in Z^+, then $a < b$ for each $a \in w_\rho$, $b \in y_\rho$. Therefore, since $w_\rho = x_\rho$ and $y_\rho = z_\rho$, then $w,x \in w_\rho$ and $y,z \in y_\rho$, so that $w < y$ and $x < z$. Thus $wy = \max\{w,y\} = y \in y_\rho$, and $xz = \max\{x,z\} = z \in z_\rho = y_\rho$, so that $(wy,xz) \in \rho$. Similarly, if $w > y$, then $(wy,xz) \in \rho$, so that ρ is a congruence on Z^+.

Conversely, if ρ is a congruence on Z^+, then let $a \varepsilon Z^+$, and consider a_ρ. Assume that there exist $x,y,z \varepsilon Z^+$ such that $x,z \varepsilon a_\rho$ and $x \leq y \leq z$, but $y \notin a_\rho$. Therefore $x \neq y$ and $y \neq z$, so that $x < y < z$. Since $x,z \varepsilon a_\rho$, then $(x,z) \varepsilon \rho$. However, $(y,y) \varepsilon \rho$, since ρ is reflexive, so that $(xy,zy) \varepsilon \rho$. Thus $(y,z) = (\max\{x,y\}, \max\{z,y\}) = (xy,zy) \varepsilon \rho$, so that $y_\rho = z_\rho = a_\rho$. This is a contradiction, since $y \notin a_\rho$. Therefore, for each $a \varepsilon Z^+$, if $x \varepsilon a_\rho$ and $z \varepsilon a_\rho$, then $y \varepsilon a_\rho$ for all $y \varepsilon Z^+$ such that $x \leq y \leq z$, and so each ρ-class is an interval in Z^+.

Theorem 3.19. Every equivalence relation is a congruence in: (1) a zero semigroup, (2) a left zero semigroup, (3) a right zero semigroup, (4) a semilattice of order 2.

Proof. Part I: Let S be a zero semigroup with zero 0, and let ρ be an equivalence relation on S. If $(a,b) \varepsilon \rho$ and $(c,d) \varepsilon \rho$, then $(ac,bd) = (0,0) \varepsilon \rho$ since ρ is reflexive, and so ρ is a congruence on S.

Part II: Let S be a left zero semigroup, and let ρ be an equivalence relation on S. If $(a,b) \varepsilon \rho$ and $(c,d) \varepsilon \rho$, then $(ac,bd) = (a,b) \varepsilon \rho$, and so ρ is a congruence on S.

Part III: Let S be a right zero semigroup, and let ρ be an equivalence relation on S. If $(a,b) \varepsilon \rho$ and $(c,d) \varepsilon \rho$, then $(ac,bd) = (c,d) \varepsilon \rho$, and so ρ is a congruence on S.

Part IV: If $S = \{a,b\}$ is a semilattice of order 2, and ρ is an equivalence relation on S, then either $\rho = S \times S$, or $\rho = \{(a,a), (b,b)\}$. If $\rho = S \times S$, then ρ is a congruence on S. If $\rho = \{(a,a), (b,b)\}$, then

1. $(a,a)*(a,a) = (aa,aa) = (a,a) \varepsilon \rho$,

2. $(b,b)*(b,b) = (bb,bb) = (b,b) \varepsilon \rho$,

3. $(a,a)*(b,b) = (ab,ab) \varepsilon \{(a,a),(b,b)\} = \rho$, and

4. $(b,b)*(a,a) = (ba,ba) = (ab,ab) \varepsilon \rho$ by part 3.

Therefore $(wy,xz) = (w,x)*(y,z) \varepsilon \rho$ for all $(w,x),(y,z) \varepsilon \rho$, so that ρ is a congruence on S. Thus every equivalence relation on S is a congruence on S.

Theorem 3.20. The set of all congruences on a semigroup S containing a fixed congruence on S is a lattice under set inclusion (an upper and a lower semilattice).

Proof. Let ρ be a congruence on a semigroup S, and let $\{\rho_\alpha\}_{\alpha\varepsilon A}$ be the set of all congruences on S containing ρ. Thus $\{\rho_\alpha\}_{\alpha\varepsilon A} \neq \phi$, since $\rho \varepsilon \{\rho_\alpha\}_{\alpha\varepsilon A}$. Let $\{\rho_{\alpha_1}, \rho_{\alpha_2}\} \subseteq \{\rho_\alpha\}_{\alpha\varepsilon A}$, and define $T \subseteq \{\rho_\alpha\}_{\alpha\varepsilon A}$ by $T = \{\rho_\alpha | \rho_\alpha$ is an upper bound of $\{\rho_{\alpha_1},\rho_{\alpha_2}\}\}$. Now $S \times S$ is a congruence on S containing ρ, and so $S \times S \varepsilon \{\rho_\alpha\}_{\alpha\varepsilon A}$. Furthermore, $\rho_{\alpha_1} \subseteq S \times S$ and $\rho_{\alpha_2} \subseteq S \times S$, so that $S \times S$ is an upper bound of $\{\rho_{\alpha_1},\rho_{\alpha_2}\}$. Therefore $S \times S \varepsilon T$, and so $T \neq \phi$. By lemma 2.20, $\beta = \bigcap_{\rho_\alpha \varepsilon T} \rho_\alpha$ is a congruence on S. Also, since $\rho \subseteq \rho_\alpha$ for all $\alpha \varepsilon A$, then $\rho \subseteq \bigcap_{\rho_\alpha \varepsilon T} \rho_\alpha = \beta$, so that $\beta \varepsilon \{\rho_\alpha\}_{\alpha\varepsilon A}$. Furthermore, since $\rho_{\alpha_1} \subseteq \rho_\alpha$ and $\rho_{\alpha_2} \subseteq \rho_\alpha$ for all $\rho_\alpha \varepsilon T$, then $\rho_{\alpha_1} \subseteq \bigcap_{\rho_\alpha \varepsilon T} \rho_\alpha = \beta$ and $\rho_{\alpha_2} \subseteq \bigcap_{\rho_\alpha \varepsilon T} \rho_\alpha = \beta$, so that β is an upper bound for for $\{\rho_{\alpha_1},\rho_{\alpha_2}\}$. Finally, if ρ_{α_0} is an upper bound of $\{\rho_{\alpha_1}, \rho_{\alpha_2}\}$, then $\rho_{\alpha_0} \varepsilon T$, and so $\beta = \bigcap_{\rho_\alpha \varepsilon T} \rho_\alpha \subseteq \rho_{\alpha_0}$. Therefore $\beta = \text{lub}\{\rho_{\alpha_1}, \rho_{\alpha_2}\}$.

Now since ρ_{α_1} and ρ_{α_2} are congruences on S, then by lemma 2.20, $\lambda = \rho_{\alpha_1} \cap \rho_{\alpha_2}$ is a congruence on S. Therefore, since $\rho \subseteq \rho_{\alpha_1}$ and $\rho \subseteq \rho_{\alpha_2}$, then $\rho \subseteq \rho_{\alpha_1} \cap \rho_{\alpha_2} = \lambda$, so that $\lambda \varepsilon \{\rho_\alpha\}_{\alpha\varepsilon A}$. Furthermore, $\lambda = \rho_{\alpha_1} \cap \rho_{\alpha_2} \subseteq \rho_{\alpha_1}$ and $\lambda = \rho_{\alpha_1} \cap \rho_{\alpha_2} \subseteq \rho_{\alpha_2}$, so that λ is a lower bound for $\{\rho_{\alpha_1}, \rho_{\alpha_2}\}$. Finally, if ρ_{α_0} is a lower bound for $\{\rho_{\alpha_1}, \rho_{\alpha_2}\}$, then $\rho_{\alpha_0} \subseteq \rho_{\alpha_1}$ and $\rho_{\alpha_0} \subseteq \rho_{\alpha_2}$, so that $\rho_{\alpha_0} \subseteq \rho_{\alpha_1} \cap \rho_{\alpha_2} = \lambda$. Therefore $\lambda = \text{glb}\{\rho_{\alpha_1}, \rho_{\alpha_2}\}$.

Thus if $\{\rho_{\alpha_1}\ \rho_{\alpha_2}\} \subseteq \{\rho_\alpha\}_{\alpha\varepsilon A}$, then there exist $\beta, \lambda \varepsilon \{\rho_\alpha\}_{\alpha\varepsilon A}$ such that $\beta = \text{lub}\{\rho_{\alpha_1}, \rho_{\alpha_2}\}$ and $\lambda = \text{glb}\{\rho_{\alpha_1}, \rho_{\alpha_2}\}$. Hence $\{\rho_\alpha\}_{\alpha\varepsilon A}$ is both an upper and a lower semilattice, and is thus a lattice.

<u>Lemma 3.21</u>. If $(R,+,\cdot)$ is a ring and $(S,*)$ is a semigroup, then let $RS = \{f:S \to R \mid |f^{-1}(R\setminus\{0\})| < \infty\}$. Define + and $\cdot$ on RS by $(f + g)(\gamma) = f(\gamma) + g(\gamma)$, and $(f \cdot g)(\gamma) = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta = \gamma}} f(\alpha)\cdot g(\beta)$, for all $\gamma \varepsilon S$. Then $(RS,+,\cdot)$ is a ring, called the semigroup ring of R by S.

<u>Proof</u>. Let $f,g,h \varepsilon RS$.

(i) If $(a,b) \varepsilon f + g$, then $a \varepsilon S$ and $b = (f + g)(a) = f(a) + g(a) \varepsilon R$, since $f(a),g(a) \varepsilon R$. Therefore $f + g \subseteq S \times R$.

(ii) If $a,b \varepsilon S$ such that $a = b$, then $f(a) = f(b)$ and $g(a) = g(b)$, so that $(f + g)(a) = f(a) + g(a) = f(b) + g(b) = (f + g)(b)$.

(iii) Since $f,g \varepsilon RS$, then there exist integers $M \geq 0$ and $N \geq 0$ such that $f^{-1}(R\setminus\{0\}) = \{x_i\}_{i=1}^{M} \subseteq S$ and

$g^{-1}(R\setminus\{0\}) = \{y_i\}_{i=1}^{N} \subseteq S$. For each i, $1 \le i \le N$, let $y_i = x_{M+i}$, so that $\{y_i\}_{i=1}^{N} = \{x_i\}_{i=M+1}^{M+N}$. Therefore, if $x \in S\setminus\{x_i\}_{i=1}^{M+N}$, then $x \notin \{x_i\}_{i=1}^{M} \cup \{y_i\}_{i=1}^{N}$, so that $f(x) = 0$ and $g(x) = 0$. Thus $(f + g)(x) = f(x) + g(x) = 0 + 0 = 0$, so that $(f + g)^{-1}(R\setminus\{0\}) \subseteq \{x_i\}_{i=1}^{M+N}$, and so $|(f + g)^{-1}(R\setminus\{0\})| \le |\{x_i\}_{i=1}^{M+N}| = |\{x_i\}_{i=1}^{M} \cup \{y_i\}_{i=1}^{N}| \le |\{x_i\}_{i=1}^{M}| + |\{y_i\}_{i=1}^{N}| = M + N < \infty$. Thus + is a closed binary operation on RS.

(iv) For each $x \in S$, $[(f + g) + h](x) = (f + g)(x) + h(x) = [f(x) + g(x)] + h(x) = f(x) + [g(x) + h(x)] = f(x) + [(g+h)(x)] = [f + (g + h)](x)$, so that $(f + g) + h = f + (g + h)$ and $(RS, +)$ is associative.

(v) For each $x \in S$, $(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$, so that $f + g = g + f$, and RS is commutative under $+$.

(vi) If $z: S \to R$ is defined by $z(x) = 0$ for all $x \in S$, then $z \in RS$, since $|z^{-1}(R\setminus\{0\})| = 0 < \infty$. Therefore, for each $f \in RS$, $(f + z)(x) = f(x) + z(x) = f(x) + 0 = f(x)$ for all $x \in S$, so that $f + z = f$. Furthermore, $z + f = f$ since RS is commutative under $+$, so that z is the identity for $+$.

(vii) Since $f \in RS$, then define $\overline{f}: S \to R$ by $\overline{f}(x) = -f(x)$ for all $x \in S$. Therefore $\overline{f}(x) = 0$ iff $-f(x) = 0$ iff $f(x) = 0$, so that $|\overline{f}^{-1}(R\setminus\{0\})| = |f^{-1}(R\setminus\{0\})| < \infty$, and $\overline{f} \in RS$. Furthermore, $(\overline{f} + f)(x) = \overline{f}(x) + f(x) = -f(x) + f(x) = 0 = z(x)$ for all $x \in S$. Therefore, for each $f \in RS$, there exists $\overline{f} \in RS$ such that $f + \overline{f} = \overline{f} + f = z$.

(viii) If $(a,b) \varepsilon f \cdot g$, then $a \varepsilon S$ and

$$b = (f \cdot g)(a) = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=a}} f(\alpha) \cdot g(\beta).$$

However, if $(\alpha,\beta) \varepsilon S \times S$ such that $\alpha*\beta = a$, then $\alpha \varepsilon S$ and $\beta \varepsilon S$, so that $f(\alpha) \varepsilon R$ and $g(\beta) \varepsilon R$, and so $f(\alpha) \cdot g(\beta) \varepsilon R$. Furthermore, since $|f^{-1}(R\setminus\{0\})| < \infty$ and $|g^{-1}(R\setminus\{0\})| < \infty$, then $|\{(\alpha,\beta) \varepsilon S \times S | \alpha*\beta = a \text{ and } f(\alpha)\cdot g(\beta) \neq 0\}| < \infty$, so that $b = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=a}} f(\alpha)\cdot g(\beta) \varepsilon R$. Therefore $f \cdot g \subseteq S \times R$.

(ix) If $a,b \varepsilon S$ such that $a = b$, then $\alpha*\beta = a$ iff $\alpha*\beta = b$ for all $(\alpha,\beta) \varepsilon S \times S$. Therefore,

$$(f \cdot g)(a) = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=a}} f(\alpha)\cdot g(\beta) = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=b}} f(\alpha)\cdot g(\beta) = (f \cdot g)(b).$$

(x) Since $f,g \varepsilon RS$, then there exist integers $M \geq 0$ and $N \geq 0$ such that $f^{-1}(R\setminus\{0\}) = \{x_i\}_{i=1}^{M} \subseteq S$ and $g^{-1}(R\setminus\{0\}) = \{y_i\}_{i+1}^{N} \subseteq S$. Therefore, if $\alpha \varepsilon S\setminus\{x_i\}_{i=1}^{M}$, then $f(\alpha) = 0$, so that $f(\alpha)\cdot g(\beta) = 0\cdot g(\beta) = 0$. Similarly, if $\beta \varepsilon S\setminus\{y_i\}_{i=1}^{N}$, then $g(\beta) = 0$, so that $f(\alpha)\cdot g(\beta) = f(\alpha)\cdot 0 = 0$. Thus, if $\gamma \varepsilon S$ such that $(f \cdot g)(\gamma) = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} f(\alpha)\cdot g(\beta) \neq 0$, then there exists $\phi \neq T \subseteq \{x_i\}_{i=1}^{M} \times \{y_i\}_{i=1}^{N}$ such that $(f \cdot g)(\gamma) = \sum_{(\alpha,\beta)\varepsilon T} f(\alpha)\cdot g(\beta)$. Since $|\{x_i\}_{i=1}^{M}| = M$ and $|\{y_i\}_{i=1}^{N}| = N$, then $|\{x_i\}_{i=1}^{M} \times \{y_i\}_{i=1}^{N}| = MN$, so that

$$|(f \cdot g)^{-1}(R\setminus\{0\})| \leq |\{P \subseteq \{x_i\}_{i=1}^{M} \times \{y_i\}_{i=1}^{N} | P \neq \phi\}| < \sum_{i=1}^{MN} \binom{MN}{i} < \infty.$$

Therefore $\cdot$ is a closed binary operation on RS.

(xi) For all $\gamma \varepsilon S$, $[(f \cdot g) \cdot h](\gamma) = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} [(f \cdot g)(\alpha)] \cdot [h(\beta)] =$

$$\sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} \left[\left(\sum_{\substack{(\lambda,\delta)\varepsilon S \times S \\ \lambda*\delta=\alpha}} [f(\lambda) \cdot g(\delta)]\right)\right] \cdot h(\beta) =$$

$$\sum_{\substack{(\lambda,\delta,\beta)\varepsilon S \times S \times S \\ \lambda*\delta*\beta=\gamma}} [f(\lambda) \cdot g(\delta) \cdot h(\beta)] = \sum_{\substack{(\alpha,\lambda,\delta)\varepsilon S \times S \times S \\ \alpha*\lambda*\delta=\gamma}} [f(\alpha) \cdot g(\lambda) \cdot h(\delta)] =$$

$$\sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} \left[f(\alpha) \cdot \left(\sum_{\substack{(\lambda,\delta)\ S \times S \\ \lambda*\delta=\beta}} [g(\lambda) \cdot h(\delta)]\right)\right] =$$

$$\sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} [f(\alpha)] \cdot [(g \cdot h)(\beta)] = [f \cdot (g \cdot h)](\gamma).$$

Therefore, $(f \cdot g) \cdot h = f \cdot (g \cdot h)$, so that $(RS, \cdot)$ is associative.

(xii) For all $\gamma \varepsilon S$, $[f \cdot (g + h)](\gamma) =$

$$\sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} [f(\alpha)] \cdot [(g + h)(\beta)] = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} f(\alpha) \cdot [g(\beta) + h(\beta)] =$$

$$\sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} ([f(\alpha) \cdot g(\beta)] + [f(\alpha) \cdot h(\beta)]) = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} f(\alpha) \cdot g(\beta) + \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} f(\alpha) \cdot h(\beta) =$$

$[(f \cdot g)(\gamma)] + [(f \cdot h)(\gamma)] = [(f \cdot g) + (f \cdot h)](\gamma)$. Therefore, $f \cdot (g + h) = (f \cdot g) + (f \cdot h)$. Similarly, for all $\gamma \varepsilon S$, $[(f + g) \cdot h](\gamma) = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} [(f + g)(\alpha)] \cdot h(\beta) =$

$$\sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} [f(\alpha) + g(\alpha)] \cdot h(\beta) = \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} ([f(\alpha) \cdot h(\beta)] + [g(\alpha) \cdot h(\beta)]) =$$

$$\sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} f(\alpha) \cdot h(\beta) + \sum_{\substack{(\alpha,\beta)\varepsilon S \times S \\ \alpha*\beta=\gamma}} g(\alpha) \cdot h(\beta) = [(f \cdot h)(\gamma)] + [(g \cdot h)(\gamma)] =$$

$[(f \cdot h) + (g \cdot h)](\gamma)$. Therefore $(f + g) \cdot h = (f \cdot h) + (g \cdot h)$, so that $\cdot$ distributes over + from the left and right in RS, and thus $(RS, +, \cdot)$ is a ring. In view of this lemma, the following example and theorem are introduced.

Example 3.22. If $(R,+,\cdot)$ is a ring, then $(R,\cdot)$ is a semigroup, called the multiplicative semigroup of R.

Embedding Theorem 3.23. Every semigroup is isomorphic to a subsemigroup of the multiplicative semigroup of some ring.

Proof. Let $(S,*)$ be a semigroup, let $(Z,+,\cdot)$ be the ring of integers, and let $(ZS, +, \cdot)$ be the semigroup ring of Z by S. Define $\theta: S \to ZS$ by $\theta(a) = f: S \to Z$, where

$$f(x) = \begin{cases} 1 \text{ if } x = a \\ 0 \text{ if } x \neq a, \text{ for all } x \in S \end{cases} \quad \text{for all } a \in S.$$

(i) If $(a,b) \in \theta$, then $a \in S$, so that $b = \theta(a) = f: S \to Z$, where $f(x) = \begin{cases} 1 \text{ if } x = a \\ 0 \text{ if } x \neq a, \end{cases}$ for all $x \in S$. Now if $(p,q) \in f$, then $p \in S$ and $q = f(p) \in \{1,0\} \subseteq Z$, so that $f \subseteq S \times Z$. Also, if $p \in S$ and $r \in S$ such that $p = r$, then either $p = a$ or $p \neq a$. If $p = a$, then $r = p = a$, so that $f(p) = f(a) = 1$, and $f(r) = f(a) = 1 = f(p)$. If $p \neq a$, then $r = p \neq a$, so that $f(p) = 0$, and $f(r) = 0 = f(p)$. In either case, if $p = r$, then $f(p) = f(r)$. Therefore $f: S \to Z$ is a well-defined function. Furthermore, $|f^{-1}(Z \setminus \{0\})| = |\{a\}| = 1 < \infty$, and so $b = \theta(a) = f \in ZS$. Thus, if $(a,b) \in \theta$, then $a \in S$ and $b \in ZS$, so that $\theta \subseteq S \times ZS$.

(ii) If $p \in S$ and $q \in S$ such that $p = q$, then $\theta(p) = f: S \to Z$, where $f(x) = \begin{cases} 1 \text{ if } x = p \\ 0 \text{ if } x \neq p, \end{cases}$ and $\theta(q) = g: S \to Z$, where $g(x) = \begin{cases} 1 \text{ if } x = q \\ 0 \text{ if } x \neq q. \end{cases}$ If $x = p$, then $x = q$, and so $f(x) = 1 = g(x)$. If $x \neq p = q$, then $x \neq q$, so that $f(x) = 0 = g(x)$. Therefore $f(x) = g(x)$ for all $x \in S$, so that $\theta(p) = f = g = \theta(q)$, and so $\theta: S \to ZS$ is well-defined.

(iii) If $a \in S$ and $b \in S$ such that $a \neq b$, then $\theta(a) = f: S \to Z$ and $\theta(b) = g: S \to Z$, where $f(x) = \begin{cases} 1 \text{ if } x = a \\ 0 \text{ if } x \neq a \end{cases}$ and $g(x) = \begin{cases} 1 \text{ if } x = b \\ 0 \text{ if } x \neq b \end{cases}$ for all $x \in S$. Therefore $f(a) = 1$, but $g(a) = 0$ since $a \neq b$, so that $\theta(a) = f \neq g = \theta(b)$. Thus θ is one-to-one.

(iv) If $a \in S$ and $b \in S$, then $\theta(ab) = f: S \to Z$, $\theta(a) = g: S \to Z$, and $\theta(b) = h: S \to Z$, where $f(x) = \begin{cases} 1 \text{ if } x = ab \\ 0 \text{ if } x \neq ab, \end{cases}$ $g(x) = \begin{cases} 1 \text{ if } x = a \\ 0 \text{ if } x \neq a, \end{cases}$ and $h(x) = \begin{cases} 1 \text{ if } x = b \\ 0 \text{ if } x \neq b. \end{cases}$ Therefore $\theta(a) \cdot \theta(b) = (g \cdot h): S \to Z$. Now

$$(g \cdot h)(ab) = \sum_{\substack{(x,y) \in S \times S \\ x*y=ab}} g(x) \cdot h(y) = g(a) \cdot h(b) + \sum_{\substack{(x,y) \in S \times S \setminus \{(a,b)\} \\ x*y=ab}} g(x) \cdot h(y).$$

However, for all $(x,y) \in S \times S \setminus \{(a,b)\}$, either $x \neq a$ or $y \neq b$. Therefore either $g(x) = 0$ or $h(y) = 0$, so that $g(x) \cdot h(y) = 0$.

Thus $(g \cdot h)(ab) = g(a) \cdot h(b) + \sum_{\substack{(x,y) \in S \times S \setminus \{(a,b)\} \\ x*y=ab}} g(x) \cdot h(y) =$

$1 \cdot 1 + \sum_{\substack{(x,y) \in S \times S \setminus \{(a,b)\} \\ x*y=ab}} (0) = 1 + 0 = 1 = f(ab)$. Furthermore,

if $p \neq ab$, then $f(p) = 0$ and $\{(x,y) \in S \times S \mid x*y=p\} \subseteq S \times S \setminus \{(a,b)\}$.

Thus $(g \cdot h)(p) = \sum_{\substack{(x,y)\in S\times S \\ x*y=p}} g(x)\cdot h(y) \leq \sum_{(x,y)\in S\times S\setminus\{(a,b)\}} g(x)\cdot h(y) = 0$,
since $g(x)\cdot h(y) = 0$ for all $(x,y) \in S\times S\setminus\{(a,b)\}$ as before, so that $(g \cdot h)(p) = 0 = f(p)$. Therefore $(g \cdot h)(ab) = f(ab)$ and $(g \cdot h)(p) = f(p)$ for all $p \in S\setminus\{ab\}$, so that $(g \cdot h)(p) = f(p)$ for all $p \in S$. Hence $\theta(a) \cdot \theta(b) = g \cdot h = f = \theta(ab)$, so that θ is a homomorphism, and thus an embedding. Since $\theta: S \to \theta(S)$ is onto as well, then $S \cong \theta(S)$.

Since $\theta: S \to ZS$, then $\theta(S) \subseteq ZS$, and $\theta(S)$ is nonempty since S is nonempty. Furthermore, if $g \in \theta(S)$ and $h \in \theta(S)$, then there exist $a \in S$ and $b \in S$ such that $\theta(a) = g$ and $\theta(b) = h$. Since θ is a homomorphism, then $g \cdot h = \theta(a)\cdot\theta(b) = \theta(ab) \in \theta(S)$ since $ab \in S$. Finally, if $f,g,h \in \theta(S)$, then there exist $a,b,c \in S$ such that $\theta(a) = f, \theta(b) = g$, and $\theta(c) = h$. Since θ is a homomorphism, then $(f \cdot g) \cdot h = [\theta(a) \cdot \theta(b)] \cdot \theta(c) = \theta(ab) \cdot \theta(c) = \theta[(ab)c] = \theta[a(bc)] = \theta(a) \cdot \theta(bc) = \theta(a) \cdot [\theta(b) \cdot \theta(c)] = f \cdot (g \cdot h)$. Therefore $(\theta(S), \cdot)$ is associative, and is thus a subsemigroup of $(ZS, \cdot)$. Thus $S \cong \theta(S)$, where $\theta(S)$ is a subsemigroup of the multiplicative semigroup $(ZS, \cdot)$ of the ring $(ZS, +, \cdot)$.

Unfortunately, it is not true that every semigroup is isomorphic to the multiplicative semigroup of some ring. The following example verifies this statement.

Example 3.24. Let S be any semigroup which contains no zero. If $(R,+,\cdot)$ is a ring, then there exists $0 \in R$ such that $0\cdot x = x\cdot 0 = 0$ for all $x \in R$. If S is isomorphic to the multiplicative semigroup $(R,\cdot)$ of $(R,+,\cdot)$, then there exists an isomorphism $f:R \to S$, so that $z = f(0) \in S$. Now for each $y \in S$, there exists $x \in R$ such that $f(x) = y$, since f is onto. Therefore, $zy = f(0)\, f(x) = f(0 \cdot x) = f(0) = z$, and $yz = f(x) f(0) = f(x \cdot 0) = f(0) = z$, so that z is a zero for S. This is a contradiction since S has no zero, and so S cannot be isomorphic to $(R,\cdot)$.

CHAPTER BIBLIOGRAPHY

1. Petrich, Mario, Introduction to Semigroups, Columbus, Ohio, Charles E. Merrill Publishing Company, 1973.

CHAPTER IV

SUBDIRECTLY IRREDUCIBLE SEMIGROUPS

Definition 4.1. If $\{S_\alpha\}_{\alpha\varepsilon A}$ is a nonempty collection of nonempty sets, then the Cartesian product of $\{S_\alpha\}_{\alpha\varepsilon A}$ is $\{f:A \to \bigcup_{\alpha\varepsilon A} S_\alpha \mid f(\alpha) \varepsilon S_\alpha$ for each $\alpha \varepsilon A\}$, and will be denoted by $\prod_{\alpha\varepsilon A} S_\alpha$. If $x \varepsilon \prod_{\alpha\varepsilon A} S_\alpha$, then $x(\alpha)$ is the α^{th} component (or coordinate) of x and will be denoted by x_α. For each $\alpha\varepsilon A$, the function $\pi_\alpha : \prod_{\alpha\varepsilon A} S_\alpha \to S_\alpha$ defined by $\pi_\alpha(x) = x_\alpha$ for all $x \varepsilon \prod_{\alpha\varepsilon A} S_\alpha$ is the α^{th} projection map of $\prod_{\alpha\varepsilon A} S_\alpha$ onto the α^{th} factor set S_α.

Lemma 4.2. Let $\{S_\alpha\}_{\alpha\varepsilon A}$ be a nonempty collection of semigroups and let $S = \prod_{\alpha\varepsilon A} S_\alpha$. Define multiplication on S as follows: if $x \varepsilon S$ and $y \varepsilon S$, then $xy = z$, where $z_\alpha = x_\alpha y_\alpha$ for all $\alpha\varepsilon A$. Then S is a semigroup, called the direct product of $\{S_\alpha\}_{\alpha\varepsilon A}$.

Proof. If $x \varepsilon S$ and $y \varepsilon S$, then $x_\alpha \varepsilon S_\alpha$ and $y_\alpha \varepsilon S_\alpha$ for all $\alpha \varepsilon A$, so that $z_\alpha = x_\alpha y_\alpha \varepsilon S_\alpha$ and $z = xy \varepsilon S$. If $x,y,z \varepsilon S$, then $x_\alpha, y_\alpha, z_\alpha \varepsilon S_\alpha$ for all $\alpha\varepsilon A$, so that $(x_\alpha y_\alpha)z_\alpha = x_\alpha(y_\alpha z_\alpha)$. Therefore $(xy)_\alpha z_\alpha = (x_\alpha y_\alpha)z_\alpha = x_\alpha(y_\alpha z_\alpha) = x_\alpha(yz)_\alpha$ for all

$\alpha\varepsilon A$, so that $(xy)z = x(yz)$. Thus multiplication in S is associative, and so S is a semigroup.

Lemma 4.3. If $\{S_\alpha\}_{\alpha\varepsilon A}$ is a nonempty collection of semigroups and $S = \prod_{\alpha\varepsilon A} S_\alpha$, then $\pi_\alpha : S \to S_\alpha$ is an onto homomorphism for each $\alpha\varepsilon A$.

Proof. If $\beta\varepsilon A$ and $(x,y)\varepsilon\pi_\beta$, then $x\varepsilon S$ and $y = \pi_\beta(x) = x_\beta = x(\beta)\varepsilon S_\beta$, and so $\pi_\beta \subseteq S \times S_\beta$. If $a\varepsilon S$ and $b\varepsilon S$ such that $a = b$, then $a_\alpha = b_\alpha$ for each $\alpha\varepsilon A$, so that $\pi_\beta(a) = a_\beta = b_\beta = \pi_\beta(b)$. Therefore, π_β is a well-defined function from S to S_β.

Let $x\varepsilon S_\beta$. Since S_α is a semigroup for each $\alpha\varepsilon A$, and thus nonempty, then select $a_\alpha\varepsilon S_\alpha$ for each $\alpha\varepsilon A$, where $a_\beta = x$. Define $a\varepsilon S$ such that $a(\alpha) = a_\alpha$ for all $\alpha\varepsilon A$, so that $\pi_\beta(a) = a_\beta = x$, and thus π_β is onto.

If $a\varepsilon S$ and $b\varepsilon S$, then $\pi_\beta(ab) = (ab)_\beta = a_\beta b_\beta = \pi_\beta(a)\pi_\beta(b)$, so that π_β is a homomorphism.

Definition 4.4. Let $\{S_\alpha\}_{\alpha\varepsilon A}$ be a collection of nontrivial semigroups. A semigroup S is a subdirect product of $\{S_\alpha\}_{\alpha\varepsilon A}$ iff there exists a subsemigroup T of $\prod_{\alpha\varepsilon A} S_\alpha$ such that $\pi_\alpha(T) = S_\alpha$ for all $\alpha\varepsilon A$ and $S \cong T$.

Definition 4.5. A nontrivial semigroup S is subdirectly irreducible iff whenever S is the subdirect product of semigroups $\{S_\alpha\}_{\alpha\varepsilon A}$ and T is a subsemigroup of $\prod_{\alpha\varepsilon A} S_\alpha$ such that $S \cong T$, then there exists $\beta\varepsilon A$ such that $\pi_\beta : T \to S_\beta$ is an isomorphism.

Definition 4.6. If σ is a congruence on a semigroup S and $x,y \in S$, then σ separates x and y iff $x_\sigma \neq y_\sigma$ (or, equivalently, $(x,y) \notin \sigma$).

Definition 4.7. A collection Σ of congruences on a semigroup S separates elements of S iff whenever $x,y \in S$ such that $x \neq y$, then there exists $\sigma \in \Sigma$ such that $x_\sigma \neq y_\sigma$.

Lemma 4.8. If Σ is a collection of congruences on a semigroup S, then Σ separates elements of S iff $\bigcap_{\sigma\in\Sigma} \sigma = \varepsilon_S$, the equality relation on S.

Proof. If Σ separates elements of S and $x,y \in S$ such that $(x,y) \notin \varepsilon_S$, then $x \neq y$. Therefore, there exists $\sigma\in\Sigma$ such that $x_\sigma \neq y_\sigma$, so that $(x,y) \notin \sigma$ and thus $(x,y) \notin \bigcap_{\sigma\in\Sigma}\sigma$. By contrapositive, if $(x,y) \in \bigcap_{\sigma\in\Sigma}\sigma$, then $(x,y) \in \varepsilon_S$, so that $\bigcap_{\sigma\in\Sigma}\sigma \subseteq \varepsilon_S$. Furthermore, if $x,y \in S$ such that $(x,y) \in \varepsilon_S$, then $x = y$. Therefore, $(x,y) = (x,x) \in \sigma$ for each $\sigma \in \Sigma$, so that $(x,y) \in \bigcap_{\sigma\in\Sigma}\sigma$ and $\varepsilon_S \subseteq \bigcap_{\sigma\in\Sigma}\sigma$. Hence $\bigcap_{\sigma\in\Sigma}\sigma = \varepsilon_S$.

Conversely, suppose $\bigcap_{\sigma\in\Sigma}\sigma = \varepsilon_S$. If $x,y \in S$, such that $x \neq y$, then $(x,y) \notin \varepsilon_S = \bigcap_{\sigma\in\Sigma}\sigma$. Therefore, there exists $\sigma\in\Sigma$ such that $(x,y) \notin \sigma$, so that $x_\sigma \neq y_\sigma$. Thus Σ separates elements of S.

Definition 4.9. If $\{S_\alpha\}_{\alpha\in A}$ is a collection of semigroups and $\beta\in A$, then the congruence σ on $\prod_{\alpha\in A} S_\alpha$ defined by $(x,y) \in \sigma$ iff $\pi_\beta(x) = \pi_\beta(y)$ for all $x,y \in \prod_{\alpha\in A} S_\alpha$ is the congruence on $\prod_{\alpha\in A} S_\alpha$ induced by π_β.

Theorem 4.10. If a semigroup S is a subdirect product of semigroups $\{S_\alpha\}_{\alpha\in A}$, then the set $\{\sigma_\alpha\}_{\alpha\in A}$ of congruences on S induced by the projection mappings $\{\pi_\alpha\}_{\alpha\varepsilon A}$ separates elements of S. Conversely, if $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ is a set of congruences on S, all different from the universal relation, which separates elements of S, then S is a subdirect product of the semigroups $\{S/\sigma_\alpha\}_{\alpha\varepsilon A}$.

Proof. If S is a subdirect product of $\{S_\alpha\}_{\alpha\varepsilon A}$, then there exists $T \subseteq \prod_{\alpha\varepsilon A} S_\alpha$ such that $S \cong T$ and $\pi_\alpha(T) = S_\alpha$ for all $\alpha\varepsilon A$. If $x \varepsilon T$ and $y \varepsilon T$ such that $x \neq y$, then there exists $\beta \varepsilon A$ such that $x_\beta \neq y_\beta$, and so $\pi_\beta(x) \neq \pi_\beta(y)$. Therefore, $(x,y) \notin \sigma_\beta$, so that $x_{\sigma_\beta} \neq y_{\sigma_\beta}$, and thus $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ separates elements of S.

Conversely, if $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ is a set of congruences on a semigroup S and $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ separates elements of S, then $\bigcap_{\alpha\varepsilon A}\sigma_\alpha = \varepsilon_S$ by lemma 4.8. Define $\theta: S \rightarrow \prod_{\alpha\varepsilon A} S/\sigma_\alpha$ by $\theta(x) = \overline{x}$, where $\overline{x}_\alpha = x_{\sigma_\alpha}$ for all $\alpha\varepsilon A$.

If $(p,q)\varepsilon\ \theta$, then $p \varepsilon S$ and $q = \theta(p) = \overline{p}$, where $q_\alpha = \overline{p}_\alpha = p_{\sigma_\alpha}$ for all $\alpha \varepsilon A$. Therefore, $q \varepsilon \prod_{\alpha\varepsilon A} S/\sigma_\alpha$, and so $\theta \subseteq S \times \prod_{\alpha\varepsilon A} S/\sigma_\alpha$. Moreover, if $x \varepsilon S$ and $y \varepsilon S$ such that $x = y$, then $[\theta(x)]_\alpha = \overline{x}_\alpha = x_{\sigma_\alpha} = y_{\sigma_\alpha}$ (since $x=y$) $= \overline{y}_\alpha = [\theta(y)]_\alpha$ for all $\alpha\varepsilon A$. Therefore, $\theta(x) = \theta(y)$, and so θ is a well-defined function.

If $x \varepsilon S$ and $y \varepsilon S$ such that $x \neq y$, then there exists $\beta \varepsilon A$ such that $x_{\sigma_\beta} \neq y_{\sigma_\beta}$ since $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ separates elements of S. Therefore, $[\theta(x)]_\beta = \overline{x}_\beta = x_{\sigma_\beta} \neq y_{\sigma_\beta} = \overline{y}_\beta = [\theta(y)]_\beta$, so that $\theta(x) \neq \theta(y)$, and hence θ is one-to-one.

If $z \varepsilon \theta(S)$, then there exists $x \varepsilon S$ such that $\theta(x) = z$, and so $\theta: S \rightarrow \theta(S)$ is onto.

If $x \varepsilon S$ and $y \varepsilon S$, then $[\theta(xy)]_\alpha = (\overline{xy})_\alpha = (xy)_{\sigma_\alpha} = (x_{\sigma_\alpha})(y_{\sigma_\alpha}) = (\overline{x}_\alpha)(\overline{y}_\alpha) = [\theta(x)]_\alpha[\theta(y)]_\alpha$ for all $\alpha \varepsilon A$. Therefore, $\theta(xy) = [\theta(x)][\theta(y)]$ for each $x,y \varepsilon S$, so that $\theta: S \rightarrow \theta(S)$ is an isomorphism, and $S \cong \theta(S)$.

Now if $y \varepsilon \theta(S)$ and $z \varepsilon \theta(S)$, then there exist $a \varepsilon S$ and $b \varepsilon S$ such that $\theta(a) = y$ and $\theta(b) = z$. Since $a \varepsilon S$ and $b \varepsilon S$ imply $ab \varepsilon S$, then $yz = [\theta(a)][\theta(b)] = \theta(ab) \varepsilon \theta(S)$.

Furthermore, since S is associative, then S/σ_α is associative for each $\alpha \varepsilon A$. Therefore, $\prod_{\alpha \varepsilon A} S/\sigma_\alpha$ is associative, and since $\theta(S) \subseteq \prod_{\alpha \varepsilon A} S/_{\sigma_\alpha}$, then $\theta(S)$ is associative. Hence, $\theta(S)$ is a subsemigroup of $\prod_{\alpha \varepsilon A} S/\sigma_\alpha$.

Finally, if $\alpha \varepsilon A$ and $x_{\sigma_\alpha} \varepsilon S/\sigma_\alpha$, then $x \varepsilon S$, and so $\theta(x) \varepsilon \theta(S)$. Furthermore, $\pi_\alpha[\theta(x)] = [\theta(x)]_\alpha = \overline{x}_\alpha = x_{\sigma_\alpha}$. Therefore, $\pi_\alpha: \theta(S) \rightarrow S/\sigma_\alpha$ is onto for each $\alpha \varepsilon A$, and so S is a subdirect product of $\{S/\sigma_\alpha\}_{\alpha \varepsilon A}$.

Lemma 4.11. The homomorphic image of a commutative or idempotent semigroup is a commutative or idempotent semigroup, respectively.

Proof. Let $(S,\cdot)$ be a semigroup, $(T,*)$ a binary system, and $f: S \rightarrow T$ a homomorphism. If $x \varepsilon f(S)$ and $y \varepsilon f(S)$, then there exists $a \varepsilon S$ and $b \varepsilon S$ such that $f(a) = x$ and $f(b) = y$. Therefore, $x*y = f(a)*f(b) = f(a\cdot b) \varepsilon f(S)$ since $a\cdot b \varepsilon S$. If $z \varepsilon f(S)$ also, then there exists $c \varepsilon S$ such that $f(c) = z$.

Therefore, $(x*y)*z = [f(a)*f(b)]*f(c) = f(a\cdot b)*f(c) = f[(a\cdot b)\cdot c] = f[a\cdot(b\cdot c)] = f(a)*f(b\cdot c) = f(a)*[f(b)*f(c)] = x*(y*z)$, and so $(f(S),*)$ is a semigroup. If $(S,\cdot)$ is commutative, then $x*y = f(a)*f(b) = f(a\cdot b) = f(b\cdot a) = f(b)*f(a) = y*x$, so that $(f(S),*)$ is commutative. If $(S,\cdot)$ is idempotent, then $x*x = f(a)*f(a) = f(a\cdot a) = f(a) = x$, so that $(f(S),*)$ is idempotent.

Theorem 4.12. The following conditions on a nontrivial semigroup S are equivalent: (i) S is subdirectly irreducible, (ii) the intersection of any collection of proper congruences on S is a proper congruence on S, and (iii) S has a least proper congruence.

Proof. Suppose S is subdirectly irreducible. If $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ is a collection of proper congruences on S such that $\bigcap_{\alpha\varepsilon A} \sigma_\alpha = \varepsilon_S$, then $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ separates elements of S by lemma 4.8. Therefore, S is the subdirect product of $\{S/\sigma_\alpha\}_{\alpha\varepsilon A}$ by theorem 4.10, so that there exists an embedding $\theta: S \to \prod_{\alpha\varepsilon A} S/\sigma_\alpha$ such that $S \cong \theta(S)$. Now for each $\alpha\varepsilon A$, $\sigma_\alpha \neq \varepsilon_S$. Therefore, if $\beta \varepsilon A$, then there exist $x \varepsilon S$ and $y \varepsilon S$, $x \neq y$, such that $(x,y) \varepsilon \sigma_\beta$, and so $x_{\sigma_\beta} = y_{\sigma_\beta}$. Furthermore, since $S \cong \theta(S)$ and $x \neq y$, then $\bar{x} = \theta(x) \neq \theta(y) = \bar{y}$. However, $\pi_\beta(\bar{x}) = \bar{x}_\beta = x_{\sigma_\beta} = y_{\sigma_\beta} = \bar{y}_\beta = \pi_\beta(\bar{y})$. Therefore, for each $\alpha \varepsilon A$, there exist $\bar{x} \varepsilon \theta(S)$ and $\bar{y} \varepsilon \theta(S)$ such that $\bar{x} \neq \bar{y}$ but $\pi_\alpha(\bar{x}) = \pi_\alpha(\bar{y})$, so that $\pi_\alpha:\theta(S) \to S/\sigma_\alpha$ is not one-to-one. Thus $\pi_\alpha:\theta(S) \to S/\sigma_\alpha$ is not an isomorphism for each $\alpha \varepsilon A$, and so S is not subdirectly irreducible. Since this contradicts the hypothesis, then $\bigcap_{\alpha\varepsilon A}\sigma_\alpha \neq \varepsilon_S$, so that $\bigcap_{\alpha\varepsilon A}\sigma_\alpha$ is a proper congruence on S by lemma 2.20.

Suppose that the intersection of any collection of proper congruences on S is a proper congruence on S. If P is the collection of all proper congruences on S, then $P \neq \phi$ since $S \times S \varepsilon P$. Therefore, $\bigcap_{\sigma\varepsilon P}\sigma$ is a proper congruence on S by hypothesis. Furthermore, if ρ is any proper congruence on S, then $\rho \varepsilon P$, so that $\bigcap_{\sigma\varepsilon P}\sigma \subseteq \rho$. Thus $\bigcap_{\sigma\varepsilon P}\sigma$ is a least proper congruence on S.

Suppose there exists a least proper congruence σ on S. If S is not subdirectly irreducible, then there exists a collection $\{S_\alpha\}_{\alpha\varepsilon A}$ of semigroups such that S is the subdirect product of $\{S_\alpha\}_{\alpha\varepsilon A}$ by the embedding $\theta: S \to \prod_{\alpha\varepsilon A} S_\alpha$, but $\pi_\alpha: \theta(S) \to S_\alpha$ is not an isomorphism for each $\alpha \varepsilon A$, where $S \cong \theta(S) \subseteq \prod_{\alpha\varepsilon A} S_\alpha$. Since $\pi_\alpha[\theta(S)] = S_\alpha$ for each $\alpha \varepsilon A$, then $\pi_\alpha: \theta(S) \to S$ is an onto homomorphism for each $\alpha \varepsilon A$ by lemma 4.3. Therefore, since π_α is not an isomorphism, then π_α is not one-to-one for each $\alpha \varepsilon A$. Let $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ be the collection of congruences induced on $\theta(S)$ by $\{\pi_\alpha\}_{\alpha\varepsilon A}$. For each $\alpha \varepsilon A$, there exist $\bar{x}, \bar{y} \varepsilon \theta(S)$ such that $\bar{x} \neq \bar{y}$, but $\pi_\alpha(\bar{x}) = \pi_\alpha(\bar{y})$ since π_α is not one-to-one. Therefore, $(\bar{x}, \bar{y}) \varepsilon \sigma_\alpha$, so that $\sigma_\alpha \neq \varepsilon_{\theta(S)}$ since $\bar{x} \neq \bar{y}$, and so σ_α is a proper congruence on $\theta(S)$ for each $\alpha \varepsilon A$. However, since S is the subdirect product of $\{S_\alpha\}_{\alpha\varepsilon A}$, then $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ separates elements of $\theta(S)$

by theorem 4.10, so that $\bigcap_{\alpha\varepsilon A}\sigma_\alpha = \varepsilon_{\theta(S)}$ by lemma 4.8. Therefore, since σ is a least proper congruence on $\theta(S)$, then $\sigma \subseteq \sigma_\alpha$ for each $\alpha \varepsilon A$, so that $\varepsilon_{\theta(S)} \subset \sigma \subseteq \bigcap_{\alpha\varepsilon A}\sigma_\alpha = \varepsilon_{\theta(S)}$. This is a contradiction, and so S is subdirectly irreducible.

Corollary 4.13. A semigroup S is a subdirect product of semigroups $\{S_\alpha\}_{\alpha\varepsilon A}$ iff there exists an onto homomorphism $f_\alpha : S \to S_\alpha$ for each $\alpha \varepsilon A$, and the family $\{\rho_\alpha\}_{\alpha\varepsilon A}$ of congruences induced by $\{f_\alpha\}_{\alpha\varepsilon A}$ separates elements of S.

Proof. If S is a subdirect product of $\{S_\alpha\}_{\alpha\varepsilon A}$, then there exists a subsemigroup T of $\prod_{\alpha\varepsilon A} S_\alpha$ such that $S \cong T$ and $\pi_\alpha(T) = S_\alpha$ for each $\alpha \varepsilon A$. Therefore, there exists an isomorphism $\theta : S \to T$ such that $T = \theta(S)$. Since $\theta : S \to T$ and $\pi_\alpha : T \to S_\alpha$ are onto homomorphisms for each $\alpha \varepsilon A$, then $\pi_\alpha \circ \theta : S \to S_\alpha$ is an onto homomorphism for each $\alpha \varepsilon A$. Let $\{\rho_\alpha\}_{\alpha\varepsilon A}$ and $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ be the families of congruences induced on S and $\theta(S)$ by $\{\pi_\alpha \circ \theta\}_{\alpha\varepsilon A}$ and $\{\pi_\alpha\}_{\alpha\varepsilon A}$, respectively. Therefore, if $x \varepsilon S$ and $y \varepsilon S$ such that $x \neq y$, then $\theta(x) \neq \theta(y)$ since θ is one-to-one. Since $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ separates elements of $\theta(S)$ by theorem 4.10, then there exists $\beta \varepsilon A$ such that $(\theta(x),\theta(y)) \notin \sigma_\beta$, so that $\pi_\beta \circ \theta(x) \neq \pi_\beta \circ \theta(y)$, and hence $(x,y) \notin \rho_\beta$. Thus $\pi_\alpha \circ \theta : S \to S_\alpha$ is an onto homomorphism for each $\alpha \varepsilon A$, and $\{\rho_\alpha\}_{\alpha\varepsilon A}$ separates elements of S.

Conversely, suppose that $f_\alpha : S \to S_\alpha$ is an onto homomorphism for each $\alpha \varepsilon A$, and the family $\{\rho_\alpha\}_{\alpha\varepsilon A}$ of congruences on S induced by $\{f_\alpha\}_{\alpha\varepsilon A}$ separates elements of S. Define

$\theta : S \to \prod_{\alpha \varepsilon A} S_\alpha$ by $[\theta(x)]_\alpha = f_\alpha(x)$ for each $x \varepsilon S$, $\alpha \varepsilon A$. If $(p,q) \varepsilon \theta$, then $p \varepsilon S$ and $q_\alpha = [\theta(p)]_\alpha = f_\alpha(p) \varepsilon S_\alpha$ for each $\alpha \varepsilon A$, so that $q \varepsilon \prod_{\alpha \varepsilon A} S_\alpha$, and so $\theta \subseteq S \times \prod_{\alpha \varepsilon A} S_\alpha$. Furthermore, if $x \varepsilon S$ and $y \varepsilon S$ such that $x = y$, then $[\theta(x)]_\alpha = f_\alpha(x) = f_\alpha(y) = [\theta(y)]_\alpha$ for each $\alpha \varepsilon A$ since f_α is well-defined, so that $\theta(x) = \theta(y)$. Therefore, θ is well-defined. If $x \varepsilon S$ and $y \varepsilon S$ such that $\theta(x) = \theta(y)$, then $f_\alpha(x) = [\theta(x)]_\alpha = [\theta(y)_\alpha] = f_\alpha(y)$ for each $\alpha \varepsilon A$. Therefore, $(x,y) \varepsilon \rho_\alpha$ for each $\alpha \varepsilon A$, so that $x = y$ since $\{\rho_\alpha\}_{\alpha \varepsilon A}$ separates elements of S. Hence θ is one-to-one. If $x \varepsilon S$ and $y \varepsilon S$, then $[\theta(xy)]_\alpha = f_\alpha(xy) = [f_\alpha(x)][f_\alpha(y)] = [\theta(x)]_\alpha [\theta(y)]_\alpha$ for each $\alpha \varepsilon A$, so that $\theta(xy) = [\theta(x)][\theta(y)]$, and so θ is a homomorphism. Thus $\theta : S \to \prod_{\alpha \varepsilon A} S_\alpha$ is an embedding, so that $S \cong \theta(S) \subseteq \prod_{\alpha \varepsilon A} S_\alpha$. Furthermore, since S is a semigroup and $S \cong \theta(S)$, then $\theta(S)$ is a semigroup by lemma 4.11, and thus a subsemigroup of $\prod_{\alpha \varepsilon A} S_\alpha$. Finally, let $\beta \varepsilon A$ and let $z \varepsilon S_\beta$. Since $f_\beta : S \to S_\beta$ is onto, then there exists $x \varepsilon S$ such that $f_\beta(x) = z$. Now $\theta(x) \varepsilon \theta(S)$, and $\pi_\beta[\theta(x)] = [\theta(x)]_\beta = f_\beta(x) = z$. Therefore, $\pi_\alpha : \theta(S) \to S_\alpha$ is onto for each $\alpha \varepsilon A$, so that $\pi_\alpha[\theta(S)] = S_\alpha$. Thus S is the subdirect product of $\{S_\alpha\}_{\alpha \varepsilon A}$.

<u>Corollary 4.14</u>. If a semigroup S is a subdirect product of semigroups $\{S_\alpha\}_{\alpha \varepsilon A}$, and S_α is a subdirect product of semigroups $\{S_{\alpha,\beta}\}_{\beta \varepsilon A_\alpha}$ for each $\alpha \varepsilon A$, then S is a subdirect product of $\{S_{\alpha,\beta}\}_{\alpha \varepsilon A, \beta \varepsilon A_\alpha}$.

Proof. If S is a subdirect product of $\{S_\alpha\}_{\alpha\varepsilon A}$, then there exists an onto homomorphism $f_\alpha: S \to S_\alpha$ for each $\alpha \varepsilon A$, and the collection $\{\rho_\alpha\}_{\alpha\varepsilon A}$ of congruences on S induced by $\{f_\alpha\}_{\alpha\varepsilon A}$ separates elements of S by corollary 4.13. Furthermore, S_α is a subdirect product of $\{S_{\alpha,\beta}\}_{\beta\varepsilon A_\alpha}$ for each $\alpha\varepsilon A$, so that if $\alpha\varepsilon A$, then there exists an onto homomorphism $g_{\alpha,\beta}: S_\alpha \to S_{\alpha,\beta}$ for each $\beta \varepsilon A_\alpha$, and the collection $\{\sigma_{\alpha,\beta}\}_{\beta\varepsilon A_\alpha}$ of congruences on S_α induced by $\{g_{\alpha,\beta}\}_{\beta\varepsilon A_\alpha}$ separates elements of S_α.

If $\alpha \varepsilon A$ and $\beta \varepsilon A_\alpha$, then $f_\alpha: S \to S_\alpha$ and $g_{\alpha,\beta}: S_\alpha \to S_{\alpha,\beta}$, so that $g_{\alpha,\beta} \circ f_\alpha : S \to S_{\alpha,\beta}$. Since f_α and $g_{\alpha,\beta}$ are onto homomorphisms, then $g_{\alpha,\beta} \circ f_\alpha$ is an onto homomorphism, and thus induces a congruence $\gamma_{\alpha,\beta}$ on S. Furthermore, if $x \varepsilon S$ and $y \varepsilon S$ such that $x \neq y$, then there exists $\alpha_\circ \varepsilon A$ such that $(x,y) \notin \rho_{\alpha_\circ}$ since $\{\rho_\alpha\}_{\alpha\varepsilon A}$ separates elements of S. Therefore, $f_{\alpha_\circ}(x) \varepsilon S_{\alpha_\circ}$ and $f_{\alpha_\circ}(y) \varepsilon S_{\alpha_\circ}$ such that $f_{\alpha_\circ}(x) \neq f_{\alpha_\circ}(y)$, and so there exists $\beta_\circ \varepsilon A_{\alpha_\circ}$ such that $(f_{\alpha_\circ}(x), f_{\alpha_\circ}(y)) \notin \sigma_{\alpha_\circ,\beta_\circ}$ since $\{\sigma_{\alpha,\beta}\}_{\beta\varepsilon A_\alpha}$ separates elements of S_α for each $\alpha \varepsilon A$. Therefore, $g_{\alpha_\circ,\beta_\circ} \circ f_{\alpha_\circ}(x) = g_{\alpha_\circ,\beta_\circ}[f_{\alpha_\circ}(x)] \neq g_{\alpha_\circ,\beta_\circ}[f_{\alpha_\circ}(y)] = g_{\alpha_\circ,\beta_\circ} \circ f_{\alpha_\circ}(y)$, so that $(x,y) \notin \gamma_{\alpha_\circ,\beta_\circ}$. Thus $g_{\alpha,\beta} \circ f_\alpha : S \to S_{\alpha,\beta}$ is an onto homomorphism for each $\alpha\varepsilon A$ and $\beta\varepsilon A_\alpha$, and the collection $\{\gamma_{\alpha,\beta}\}_{\alpha\varepsilon A,\beta\varepsilon A_\alpha}$ of congruences on S induced by $\{g_{\alpha,\beta} \circ f_\alpha\}_{\alpha\varepsilon A,\beta\varepsilon A_\alpha}$ separates elements of S, so that S is the subdirect product of $\{S_{\alpha,\beta}\}_{\alpha\varepsilon A,\beta\varepsilon A_\alpha}$ by corollary 4.13.

The proof of the following theorem is found on p. 24 of Introduction to Semigroups, by Mario Petrich.

Theorem 4.15. Every semigroup is a subdirect product of subdirectly irreducible semigroups.

Proof. If S is a semigroup, $a \in S$, and $b \in S$ such that $a \neq b$, then define $M(a,b) = \{\rho \text{ congruence on } S \mid \rho \text{ separates } a \text{ and } b\}$. Therefore, $M(a,b) \neq \phi$ since $\varepsilon_S \in M(a,b)$. Let Γ be a chain in $M(a,b)$, and define $\lambda = \bigcup_{\rho \in \Gamma} \rho \subseteq S \times S$. If $x \in S$, then $(x,x) \in \rho$ for each $\rho \in \Gamma$, so that $(x,x) \in \bigcup_{\rho \in \Gamma} \rho = \lambda$ and λ is reflexive. If $x \in S$ and $y \in S$ such that $(x,y) \in \lambda$, then there exists $\rho \in \Gamma$ such that $(x,y) \in \rho$. Therefore, $(y,x) \in \rho \subseteq \bigcup_{\rho \in \Gamma} \rho = \lambda$, and so λ is symmetric. If $x,y,z \in S$ such that $(x,y) \in \lambda$ and $(y,z) \in \lambda$, then there exist $\rho_1 \in \Gamma$ and $\rho_2 \in \Gamma$, such that $(x,y) \in \rho_1$ and $(y,z) \in \rho_2$. Since Γ is a chain, then either $\rho_1 \subseteq \rho_2$ or $\rho_2 \subseteq \rho_1$. If $\rho_1 \subseteq \rho_2$, then $(x,y) \in \rho_2$ and $(y,z) \in \rho_2$, so that $(x,z) \in \rho_2 \subseteq \bigcup_{\rho \in \Gamma} \rho = \lambda$; and if $\rho_2 \subseteq \rho_1$, then $(x,y) \in \rho_1$ and $(y,z) \in \rho_1$, so that $(x,z) \in \rho_1 \subseteq \bigcup_{\rho \in \Gamma} \rho = \lambda$. Therefore, if $(x,y) \in \lambda$ and $(y,z) \in \lambda$, then $(x,z) \in \lambda$, and so λ is an equivalence relation on S. If $(w,x) \in \lambda$ and $(y,z) \in \lambda$, then there exists $\rho_3 \in \Gamma$ and $\rho_4 \in \Gamma$ such that $(w,x) \in \rho_3$ and $(y,z) \in \rho_4$. As before, either $\rho_3 \subseteq \rho_4$ or $\rho_4 \subseteq \rho_3$ since Γ is a chain. If $\rho_3 \subseteq \rho_4$, then $(w,x) \in \rho_4$ and $(y,z) \in \rho_4$, so that $(wy,xz) \in \rho_4 \subseteq \bigcup_{\rho \in \Gamma} \rho = \lambda$; and if $\rho_4 \subseteq \rho_3$, then $(w,x) \in \rho_3$ and $(y,z) \in \rho_3$, so that

$(wy, xz) \in \rho_3 \subseteq \bigcup_{\rho \in \Gamma} \rho = \lambda$. Thus λ is a congruence on S. Furthermore, since ρ separates a and b for each $\rho \in \Gamma$, then $(a,b) \notin \rho$ for each $\rho \in \Gamma$, so that $(a,b) \notin \bigcup_{\rho \in \Gamma} \rho = \lambda$. Therefore, λ separates a and b, and so $\lambda \in M(a,b)$. Obviously, $\rho \subseteq \bigcup_{\rho \in \Gamma} \rho = \lambda$ for each $\rho \in \Gamma$, so that λ is an upper bound for Γ. Thus every chain Γ in $M(a,b)$ has an upper bound $\lambda \in M(a,b)$, so that $M(a,b)$ has a maximal element $\sigma(a,b)$ by Zorn's Lemma. Hence, for each $(x,y) \in S \times S$ such that $x \neq y$, there exists a maximal congruence $\sigma(x,y)$ on S which separates x and y. Define $A = \{\sigma(x,y) \mid x \in S, y \in S, x \neq y\}$, so that A is a family of congruences on S which separates elements of S. Therefore, S is a subdirect product of semigroups $\{S/_{\sigma(x,y)}\}_{\sigma(x,y) \in A}$ by theorem 4.10.

Now if $a \in S$ and $b \in S$ such that $a \neq b$, then define $P = \{\rho \text{ congruence on } S \mid \sigma(a,b) \subseteq \rho\}$. For each $\rho \in P$, define ρ' on $S/_{\sigma(a,b)}$ by $(x_{\sigma(a,b)}, y_{\sigma(a,b)}) \in \rho'$ iff $(x,y) \in \rho$, for all $x \in S$, $y \in S$. Define $P' = \{\rho' \mid \rho \in P\}$. By lemma 2.26, $f: P \to P'$ defined by $f(\rho) = \rho'$ for all $\rho \in P$ is a one-to-one, order-preserving function, with $f(\sigma(a,b)) = \varepsilon_{S/_{\sigma(a,b)}}$. Therefore, if $\rho \in P$ such that $\sigma(a,b) \subset \rho$, then $\rho \neq \sigma(a,b)$, so that $\rho' = f(\rho) \neq f(\sigma(a,b)) = \varepsilon_{S/_{\sigma(a,b)}}$, since f is one-to-one. Thus $f: P \setminus \{\sigma(a,b)\} \to P' \setminus \{\varepsilon_{S/_{\sigma(a,b)}}\}$, so that

$$f: \{\rho \text{ congruence on } S \mid \sigma(a,b) \subset \rho\} \to \{\rho' \text{ congruence on } S/_{\sigma(a,b)} \mid \rho' \neq \varepsilon_{S/_{\sigma(a,b)}}\}.$$

Define $\alpha = \bigcap_{\rho \varepsilon P \setminus \{\sigma(a,b)\}} \rho$, $\alpha' = \bigcap_{\rho' \varepsilon P' \setminus \{\varepsilon_{S/\sigma(a,b)}\}} \rho'$.

Since f is one-to-one, then

$$f(\alpha) = f[\bigcap_{\rho \varepsilon P\setminus\{\sigma(a,b)\}} \rho] = \bigcap_{\rho \varepsilon P\setminus\{\sigma(a,b)\}} f(\rho) = \bigcap_{\rho' \varepsilon P'\setminus\{\varepsilon_{S/\sigma(a,b)}\}} \rho' = \alpha'.$$

However, if $\rho \varepsilon P\setminus\{\sigma(a,b)\}$, then $\sigma(a,b) \subset \rho$, so that ρ does not separate a and b, since $\sigma(a,b)$ is maximal. Thus $a_\rho = b_\rho$, and so $(a,b) \varepsilon \rho$. Therefore, $(a,b) \varepsilon \rho$ for all $\rho \varepsilon P\setminus\{\sigma(a,b)\}$, so that $(a,b) \varepsilon \bigcap_{\rho \varepsilon P\setminus\{\sigma(a,b)\}} \rho = \alpha$. Hence α does not separate a and b, so that $\alpha \neq \sigma(a,b)$. However, $\sigma(a,b) \subset \rho$ for all $\rho \varepsilon P\setminus\{\sigma(a,b)\}$, so that $\sigma(a,b) \subseteq \bigcap_{\rho \varepsilon P\setminus\{\sigma(a,b)\}} \rho = \alpha$. Thus $\sigma(a,b) \subset \alpha$, so that $\alpha \varepsilon P\setminus\{\sigma(a,b)\}$, and so

$$\alpha' \neq \bigcap_{\rho' \varepsilon P'\setminus\{\varepsilon_{S/\sigma(a,b)}\}} \rho' = f(\alpha) \varepsilon P'\setminus\{\varepsilon_{S/\sigma(a,b)}\}.$$

Therefore, the intersection α' of all proper congruences ρ' on $S/_{\sigma(a,b)}$ is a proper congruence on $S/_{\sigma(a,b)}$, so that $S/_{\sigma(a,b)}$ is subdirectly irreducible by theorem 4.12. Thus S is a subdirect product of $\{S/_{\sigma(x,y)}\}_{\sigma(x,y)\varepsilon A}$, where $S/_{\sigma(x,y)}$ is subdirectly irreducible for each $\sigma(x,y) \varepsilon A$.

Corollary 4.16. Every commutative or idempotent semigroup is a subdirect product of subdirectly irreducible commutative or idempotent semigroups, respectively.

Proof. If S is a semigroup, then S is a subdirect product of subdirectly irreducible semigroups $\{S_\alpha\}_{\alpha\varepsilon A}$ by theorem 4.15. By corollary 4.13, there exists a collection $\{f_\alpha\}_{\alpha \varepsilon A}$ such that $f_\alpha : S \to S_\alpha$ is a homomorphism of S onto S_α for each $\alpha \varepsilon A$. Therefore, $f_\alpha(S) = S_\alpha$ for each $\alpha \varepsilon A$, so that S_α is a homomorphic image of S for each $\alpha \varepsilon A$. Thus if S is commutative or idempotent, then S_α is commutative or idempotent, respectively, by lemma 4.11.

The following theorem characterizes all subdirectly irreducible finite abelian groups.

Theorem 4.17. If G is a finite abelian group, then G is subdirectly irreducible iff G is cyclic and there exist $p \varepsilon Z^+$ and $n \varepsilon Z^+$ such that p is prime and $|G| = p^n$.

Proof. Suppose G is cyclic, $p \varepsilon Z^+$, and $n \varepsilon Z^+$ such that p is a prime and $|G| = p^n$. Since G is cyclic, then there exists $a \varepsilon G$ such that $G = \langle a \rangle$, the subgroup generated by $\{a\}$.

Case I: Suppose n = 1. If H is a subgroup of G, then H is also cyclic, so that there exists $x \varepsilon H$ such that $H = \langle x \rangle$. If x = e, the identity for G, then $H = \langle x \rangle = \{e\}$. If $x \neq e$, then x is a generator for G, since G is of prime order, so that $H = \langle x \rangle = G$. Thus the only nontrivial normal subgroup (and hence proper congruence, by theorem 2.19) of G is G itself. Therefore, G is the least proper congruence on G, and so G is subdirectly irreducible by theorem 4.12.

Case II: Suppose n >1. By Sylow's theorem, there exists a normal subgroup H of $\langle a \rangle$ such that $|H| = p$. If $m \varepsilon Z^+$ and $a^m = e$, then $m \geq p^n$ since $|\langle a \rangle| = p^n$. However, $H \neq \{e\}$, and so there exists $a^w \varepsilon \langle a \rangle \backslash \{e\} = \{a^i\}_{i=1}^{p^n - 1}$ such that $a^w \in H$, where $w \leq p^n - 1 < p^n \leq m$. Thus if $m \in Z^+$ and $a^m = e$, then there exists $w \in Z^+$ such that $w < m$ and $a^w \in H$. By contrapositive, if m is the smallest positive integer such that $a^m \in H$, then $a^m \neq e$. Since H is of prime order, then any non-identity element of H is a generator for H. Therefore, $H = \langle a^m \rangle = \{(a^m)^i\}_{i=1}^{p}$, where $1 \leq im \leq p^n$ for all i, $1 \leq i \leq p$. Since $|\langle a^m \rangle| = |H| = p$, then $a^{mp} = (a^m)^p = e$.

Assume that $m > p^{n-1}$. Then $mp > p^n$. Let q be the least positive integer in $\{1, 2, \cdots, p\}$ such that $mq > p^n$. Therefore there exists $t \in Z^+$ and $r \in Z^+$, $0 \leq r < m$, such that $mq = tp^n + r$. If $r = 0$, then $mq = tp^n$, so that $m = \frac{tp^n}{q}$ and $a^m = (a^{p^n})^{\frac{t}{q}} = (e)^{\frac{t}{q}} = e$. However, $a^m \neq e$, so that $r \neq 0$, and so $0 < r < m$. Since $mq = tp^n + r$, then $mq - tp^n = r$. Now $a^{mq} = (a^m)^q \in H$ since $a^m \in H$, and $a^{-tp^n} = (a^{p^n})^{-t} = e^{-t} = e \in H$. Therefore, $a^r = a^{mq - tp^n} = a^{mq} \cdot a^{-tp^n} \in H$, where $0 < r < m$. This is a contradiction, since m is the smallest positive integer such that $a^m \in H$. Thus $m \leq p^{n-1}$, so that $mp \leq p^{n-1}p = p^n$. Furthermore, $|\langle a^m \rangle| = |H| = p$, so that $a^{mp} = e$. However, $|\langle a \rangle| = p^n$, so that p^n is the smallest positive integer such that $a^{p^n} = e$, and so $mp \geq p^n$. Therefore, $mp = p^n$, so that $m = p^{n-1}$, and so $H = \langle a^m \rangle = \langle a^{p^{n-1}} \rangle$. Thus $\langle a^{p^{n-1}} \rangle$ is the unique normal subgroup of $\langle a \rangle$ of order p.

Now if D is a normal subgroup of $\langle a \rangle$, then $|D|$ divides $|\langle a \rangle|$ by Lagrange's theorem. Therefore, $|D|$ divides p^n so that $|D| = p^t$ for some $t \in Z$, $0 \leq t \leq n$. Furthermore, if D is nontrivial, the $p^t = |D| > 1$, so that $1 \leq t \leq n$. Thus D has a normal subgroup C such that $|C| = p$ by Sylow's theorem. But then C is a normal subgroup of $<a>$. Since $<a^{p^{n-1}}>$ is the unique normal subgroup of $<a>$ of order p, then $<a^{p^{n-1}}> = C \subseteq D$. Therefore, if D is any nontrivial normal subgroup of $<a>$, then $<a^{p^{n-1}}> \subseteq D$. Hence $<a^{p^{n-1}}>$ is the least nontrivial normal subgroup of $<a> = G$, so that there corresponds a least proper congruence on G by theorem 2.19, and so G is subdirectly irreducible by theorem 4.12.

Conversely, suppose G is a subdirectly irreducible finite abelian group with identity e. If G is not of order p^n, where p is prime and $n \in Z^+$, then there exist distinct primes p and q such that p divides $|G|$ and q divides $|G|$. By Cauchy's theorem, there exist normal subgroups H and K of G such that $|H| = p$ and $|K| = q$. Since H and K are of prime order, then H and K are cyclic, and so there exist $a \in G$ and $b \in G$ such that $H = <a>$ and $K = <b>$. Now $e \in H \cap K$. However, if there exists $x \in H \cap K$ such that $x \neq e$, then x is a generator for H and K. Therefore, $H = <x> = K$, and so $p = |H| = |K| = q$. This is a contradiction since p and q are distinct primes, so that $H \cap K = \{e\}$, and so $\{H,K\}$ is a collection of nontrivial normal subgroups of G whose intersection is the trivial normal subgroup $\{e\}$ of G. Hence, there exists a collection of corresponding proper congruences on G whose intersection is the improper congruence ε_G on G, and so G is not subdirectly irreducible by theorem 4.12. Since this contradicts the original hypothesis, then $|G| = p^n$, where p is a prime and $n \in Z^+$.

If Q is a subdirectly irreducible finite abelian group and $|Q| = p^1$, then Q is of prime order, and so Q is cyclic. Now assume that for each $i \in Z^+$, $1 \leq i \leq k-1$, if Q is a subdirectly irreducible finite abelian group and $|Q| = p^i$, then Q is cyclic. Let Q be a subdirectly irreducible finite abelian group such that $|Q| = p^k$. Define $H = \{x^p | x \in Q\}$, so that $H \subseteq Q$. Define $f:Q \to H$ by $f(x) = x^p$ for each $x \in Q$. Since $Q \neq \phi$, then there exists $x \in Q$, so that $f(x) = x^p \in H$. Therefore, $(x,x^p) \in f$, and so $f \neq \phi$. Moreover, if $(x,y) \in f$, then $x \in Q$ and $y = f(x) = x^p \in H$, so that $f \subseteq Q \times H$. Furthermore, if $x \in Q$ and $y \in Q$ such that $x = y$, then $f(x) = x^p = y^p = f(y)$, and so f is a well-defined function. If $z \in H$, then there exists $x \in Q$ such that $z = x^p = f(x)$, so that f is onto H. Finally, if $x \in Q$ and $y \in Q$, then $f(xy) = (xy)^p = x^p y^p$ (since Q is abelian) $= f(x)\, f(y)$. Therefore, $f:Q \to H$ is a well-defined, onto homomorphism, and so $H = f(Q)$ is a group since Q is a group. Hence, H is a subgroup of G. Furthermore, since Q is subdirectly irreducible and $|Q| = p^k$, then Q has a least proper congruence, and so there exists a corresponding unique nontrivial normal subgroup T of Q such that $|T| = p$. Since T is of prime order, then any non-identity element of T is a generator for T. Since $|T| = p$, then $f(x) = x^p = e$ for all $x \in T$, so that $T \subseteq \ker(f)$. Assume there exists $x \in Q \backslash T$ such that $x \in \ker(f)$. Therefore

$x^p = f(x) = e$, so that $|\langle x\rangle| \leq p$. Since $|Q| = p^k$, then $|\langle x\rangle|$ divides p^k, so that either $|\langle x\rangle| = 1$ or $|\langle x\rangle| = p$. If $|\langle x\rangle| = 1$, then $\langle x\rangle = \{e\}$, so that $x = e \in T$. This is a contradiction since $x \in Q\backslash T$. Therefore, $|\langle x\rangle| = p$. Since $x \in \langle x\rangle$ but $x \notin T$, then $\langle x\rangle \neq T$. Furthermore, $\langle x\rangle$ is a normal subgroup of Q since Q is abelian. Thus $\langle x\rangle$ and T are distinct normal subgroups of Q of order p. However, this is also a contradiction since T is the unique normal subgroup of Q of order p. Therefore, if $x \in Q\backslash T$, then $x \notin \ker(f)$, so that $\ker(f) \subseteq T$. Hence $T = \ker(f)$. Since $f: Q \to H$ is an onto homomorphism, then $H \cong Q/\ker(f)$ by the fundamental theorem of group homomorphisms, so that

$$|H| = |Q/\ker(f)| = |Q/T| = \frac{|Q|}{|T|} = \frac{p^k}{p} = p^{k-1}.$$

Assume that H is not subdirectly irreducible, so that there exists a collection $\{\rho_\alpha\}_{\alpha\varepsilon A}$ of proper congruences on H such that $\bigcap_{\alpha\varepsilon A} \rho_\alpha = \varepsilon_H$. Therefore, there exists a collection $\{B_\alpha\}_{\alpha\varepsilon A}$ of corresponding nontrival normal subgroups of H such that $\bigcap_{\alpha\varepsilon A} B_\alpha = \{e\}$ by theorem 2.19. However, since B_α is a nontrivial subgroup of H for each $\alpha \varepsilon A$, and H is a subgroup of Q, then $\{B_\alpha\}_{\alpha\varepsilon A}$ is a collection of nontrivial subgroups of Q. Furthermore, B_α is normal in Q for all $\alpha \varepsilon A$ since Q is abelian. Therefore, since $\bigcap_{\alpha\varepsilon A} B_\alpha = \{e\}$, then there exists a collection $\{\sigma_\alpha\}_{\alpha\varepsilon A}$ of corresponding proper congruences on Q such that $\bigcap_{\alpha\varepsilon A} \sigma_\alpha = \varepsilon_Q$ by theorem 2.19, and so Q is not subdirectly irreducible. This contradicts the hypothesis, and so H is subdirectly irreducible. Since $|H| = p^{k-1}$, then H is cyclic by hypothesis. Therefore, there exists $x \varepsilon Q$ such that $x^p \varepsilon H$ and $\langle x^p \rangle = H$, so that $|\langle x^p \rangle| = |H| = p^{k-1}$, and so $x^{p^k} = (x^p)^{p^{k-1}} = e$. Since $|\langle x \rangle|$ divides $|Q| = p^k$, then there exists $t \varepsilon Z$, $0 \leq t \leq k$, such that $|\langle x \rangle| = p^t$. If $t < k$, then $t-1 < k-1$, and so $p^{t-1} < p^{k-1}$. Therefore, since $|\langle x^p \rangle| = p^{k-1}$, then $x^{p^t} = (x^p)^{p^{t-1}} \neq e$. This is a contradiction, since $|\langle x \rangle| = p^t$, and so $t = k$. Hence $|\langle x \rangle| = p^k = |Q|$, so that $\langle x \rangle = Q$, and so Q is cyclic. Therefore, by mathematical induction, if Q is a subdirectly irreducible finite abelian group, p is a prime, $m \varepsilon Z^+$, and $|Q| = p^m$, then Q is cyclic. Thus, since G is a subdirectly irreducible finite abelian group and $|G| = p^n$, where p is a prime and $n \varepsilon Z^+$, then G is cyclic.

Theorem 4.18. A zero semigroup is subdirectly irreducible iff $|S| = 2$.

Proof. Suppose S is a subdirectly irreducible zero semigroup with zero 0. If $|S| \neq 2$, then either $|S| = 1$ or $|S| \geq 3$. If $|S| = 1$, then there does not exist a proper congruence on S, and so S is not subdirectly irreducible. This is a contradiction, and so $|S| \neq 1$. If $|S| \geq 3$, then there exists $a \varepsilon S$ and $b \varepsilon S$ such that $a \neq 0$, $b \neq 0$, and $a \neq b$. Define relations ρ and γ on S by

$$x_\rho = \begin{cases} \{x\} \text{ for each } x \varepsilon S \backslash \{a,0\} \\ \{a,0\} \text{ for each } x \varepsilon \{a,0\} \end{cases}$$

and

$$x_\gamma = \begin{cases} \{x\} \text{ for each } x \in S \setminus \{b,0\} \\ \{b,0\} \text{ for each } x \in \{b,0\}. \end{cases}$$

Since ρ partitions S, then ρ induces an equivalence relation on S. Furthermore, if $w,x,y,z \in S$ such that $(w,x) \in \rho$ and $(y,z) \in \rho$, then $(wy,xz) = (0,0) \in \rho$, and so ρ is a congruence on S. Similarly, γ is also a congruence on S. Now $\rho \setminus \varepsilon_S = \{(a,0),(0,a)\}$ and $\gamma \setminus \varepsilon_S = \{(b,0),(0,b)\}$. Since $a \neq b$ and $a \neq 0$, then $(a,0) \notin \gamma \setminus \varepsilon_S$ and $(0,a) \notin \gamma \setminus \varepsilon_S$, so that $(\rho \setminus \varepsilon_S) \cap (\gamma \setminus \varepsilon_S) = \phi$, and thus $\rho \cap \gamma = \varepsilon_S$. Hence, ρ and γ are proper congruences on S whose intersection is an improper congruence on S, and so S is not subdirectly irreducible. This contradicts the hypothesis, so that $|S| < 3$. Therefore, since $|S| \neq 1$ and $|S| < 3$, then $|S| = 2$.

Conversely, if $|S| = 2$, then the universal relation $w_S = S \times S$ is the only proper congruence on S, and is thus the least proper congruence on S. Therefore, S is subdirectly irreducible by theorem 4.12.

Lemma 4.19. Every cyclic semigroup S with zero z is finite. Furthermore, if N is the smallest positive integer t such that $a^t = z$, where $\langle a \rangle = S$, then $|S| = N$.

Proof. Since S is cyclic, then there exists $a \in S$ such that $\langle a \rangle = S$. If z is the zero for S, then $z \in \langle a \rangle$, and so there exists $n \in Z^+$ such that $a^n = z$. For each $m > n$, $m - n > 0$, so that $a^{m-n} \in S$. Therefore, $a^m = a^{n+(m-n)} = a^n \cdot a^{m-n} = z \cdot a^{m-n} = z$, so that $|S| \leq n$, and thus S is finite.

Define $B = \{x \in Z^+ | a^x = z\}$, so that $B \neq \phi$ since $n \in B$. Since Z^+ is well-ordered, then there exists a least element N of B. Therefore, $a^m = z$ for each $m \geq N$, so that $|S| \leq N$. Assume that there exist $i \in Z^+$ and $j \in Z^+$ such that $1 \leq i < j \leq N$ and $a^i = a^j$. Since N is the least element of B and $i < j$, then $j \neq N$. Hence, $1 \leq i < j < N$, so that $N-j > 0$ and $a^{N-j} \in S$. Therefore,
$z = a^N = a^{j+N-j} = a^j \cdot a^{N-j} = a^i \cdot a^{N-j} = a^{i+N-j} = a^{N-(j-i)}$,
and so $N-(j-i) \in B$. However, $j > i$, so that $j-i > 0$, and $N-(j-i) < N$. This is a contradiction, since N is the least element of B. Therefore, if $i \in Z^+$ and $j \in Z^+$, such that $1 \leq i \leq N$, $1 \leq j \leq N$, and $i \neq j$, then $a^i \neq a^j$, and so $|S| = N$.

Theorem 4.20. Every nontrivial cyclic semigroup with zero is subdirectly irreducible.

Proof. Let S be a nontrivial cyclic semigroup with zero z; then there exists $a \in S$ such that $\langle a \rangle = S$. By lemma 4.19, S is finite, and if n is the smallest positive integer t such that $a^t = z$, then $|S| = n$, so that $S = \{a^1, a^2, \cdots, a^{n-1}, a^n\}$. Define ρ on S by

$$a_\rho^i = \begin{cases} \{a^i\}, & 1 \leq i \leq n-2 \\ \{a^{n-1}, a^n\}, & n-1 \leq i \leq n. \end{cases}$$

Since ρ partitions S, then ρ induces an equivalence relation on S. Suppose $a^i, a^j, a^k, a^m \in S$ such that $(a^i, a^j) \in \rho$, and $(a^k, a^m) \in \rho$. If $1 \leq i \leq n-2$ and $1 \leq k \leq n-2$, then $\{a^i\} = a_\rho^i = a_\rho^j = \{a^j\}$ and $\{a^k\} = a_\rho^k = a_\rho^m = \{a^m\}$. Therefore, $i = j$ and $k = m$, so that $i + k = j + m$. Hence, $a^i a^k =$

$a^{i+k} = a^{j+m} = a^j a^m$, and so $(a^i a^k, a^j a^m) \varepsilon \rho$ since ρ is reflexive. If $i \geq n-1$, then $j \geq n-1$ since $(a^i, a^j) \varepsilon \rho$. Since $k \geq 1$ and $m \geq 1$, then $i+k \geq n$ and $j+m \geq n$, so that $a^i a^k = a^{i+k} = z = a^{j+m} = a^j a^m$, and hence $(a^i a^k, a^j a^m) \varepsilon \rho$. Similarly, if $k \geq n-1$, then $(a^i a^k, a^j a^m) \varepsilon \rho$. Thus ρ is a congruence on S. Furthermore, since $n-1 < n$, and n is the least positive integer t such that $a^t = z$, then $a^{n-1} \neq z = a^n$. Therefore, since $(a^{n-1}, a^n) \varepsilon \rho$, then ρ is a proper congruence on S. Note that $\rho = \varepsilon_S \cup \{(a^{n-1}, a^n), (a^n, a^{n-1})\}$. Now if γ is any proper congruence on S, then there exist $i \varepsilon Z^+$ and $j \varepsilon Z^+$ such that $1 \leq i < j \leq n$ and $(a^i, a^j) \varepsilon \rho$. Since $i < j \leq n$, then $i \leq n-1$. If $i = n-1$, then $j = n$, since $i < j$. Therefore, since $(a^i, a^j) \varepsilon \gamma$, then $(a^{n-1}, a^n) \varepsilon \gamma$, and so $(a^n, a^{n-1}) \varepsilon \gamma$ since γ is symmetric. Hence, $\varepsilon_S \subseteq \gamma$, $(a^{n-1}, a^n) \varepsilon \gamma$, and $(a^n, a^{n-1}) \varepsilon \gamma$, so that $\rho \subseteq \gamma$. On the other hand, if $i < n-1$, then $n-1-i > 0$, so that $a^{n-1-i} \varepsilon S$, and hence $(a^{n-1-i}, a^{n-1-i}) \varepsilon \gamma$ since γ is reflexive. Since $(a^i, a^j) \varepsilon \gamma$ as well, then $(a^{n-1}, a^{n-1+j-i}) = (a^i a^{n-1-i}, a^j a^{n-1-i}) \varepsilon \gamma$. However, $j-i > 0$ since $i < j$, so that $n-1+j-i > n-1$, and hence $n-1+j-i \geq n$. Therefore, $a^{n-1+j-i} = z = a^n$, so that $(a^{n-1}, a^n) = (a^{n-1}, a^{n-1+j-i}) \varepsilon \gamma$, and so $(a^n, a^{n-1}) \varepsilon \gamma$, since γ is symmetric. Since $\varepsilon_S \subseteq \gamma$, $(a^{n-1}, a^n) \varepsilon \gamma$, and $(a^n, a^{n-1}) \varepsilon \gamma$, then $\rho \subseteq \gamma$ as before. Thus ρ is a proper congruence on S, and if γ is any proper congruence on S, then $\rho \subseteq \gamma$. Hence ρ is the least proper congruence on S, and so S is subdirectly irreducible.

<u>Lemma 4.21</u>. Let S be a nontrivial semigroup with zero 0. If N is an ideal of S, and ρ is the equivalence relation on S defined by

$$x_\rho = \begin{cases} N & \text{for each } x \in N \\ \{x\} & \text{for each } x \in S\setminus N, \end{cases}$$

then ρ is a congruence on S with $0_\rho = N$. Conversely, if ρ is a congruence on S, then 0_ρ is an ideal of S.

<u>Proof</u>. Suppose N is an ideal of S and define ρ on S by

$$x_\rho = \begin{cases} N & \text{for each } x \in N \\ \{x\} & \text{for each } x \in S\setminus N. \end{cases}$$

Since ρ partitions S, then ρ defines an equivalence relation on S. If $w,x,y,z \in S$ such that $(w,x) \in \rho$ and $(y,z) \in \rho$, then $w_\rho = x_\rho$ and $y_\rho = z_\rho$. If $w \notin N$ and $y \notin N$, then $\{w\} = w_\rho = x_\rho$ and $\{y\} = y_\rho = z_\rho$, so that $x = w$ and $z = y$. Therefore, $wy = xz$, and so $(wy,xz) \in \rho$. If $w \in N$, then $N = w_\rho = x_\rho$, so that $x \in N$ as well. Therefore, $wy \in N$ and $xz \in N$ since N is an ideal, so that $(wy)_\rho = N = (xz)_\rho$, and thus $(wy,xz) \in \rho$. Similarly, if $y \in N$, then $(wy,xz) \in \rho$. Hence, in any case, if $(w,x) \in \rho$ and $(y,z) \in \rho$, then $(wy,xz) \in \rho$, and so ρ is a congruence on S. Furthermore, since N is an ideal in S, then there exists $x \in N$, so that $0 = 0x \in N$, and thus $0_\rho = N$.

Conversely, if ρ is a congruence on S, then let $x \in S$ and $y \in 0_\rho$, so that $(y,0) \in \rho$. Since $(x,x) \in \rho$ also, then $(xy,0) = (xy,x0) \in \rho$ and $(yx,0) = (yx,0x) \in \rho$. Therefore, $xy \in 0_\rho$ and $yx \in 0_\rho$, and so 0_ρ is an ideal in S.

Definition 4.22. The congruence ρ on S defined in lemma 4.21 is the congruence on S induced by the ideal N.

Definition 4.23. An ideal N of a semigroup S is degenerate iff $|N| = 1$; N is nondegenerate iff $|N| > 1$.

Corollary 4.24. If N is a nondegenerate ideal of a semigroup S with zero 0, then the congruence ρ on S induced by N is a proper congruence.

Proof. Since N is an ideal of S, then $0 \in N$. However, $N \neq \{0\}$ since N is nondegenerate, and so there exists $a \in S\setminus\{0\}$ such that $\{0,a\} \subseteq N$. Therefore, if ρ is the congruence on S induced by N, then $0_\rho = N = a_\rho$. Hence $(0,a) \in \rho$, while $0 \neq a$ since $a \in S\setminus\{0\}$, and so $\rho \neq \varepsilon_S$. Thus, ρ is a proper congruence on S.

Theorem 4.25. If S is a semigroup with zero 0 such that: (1) there exists a least nondegenerate ideal of S, and (2) 0_ρ is a nondegenerate ideal of S whenever ρ is a proper congruence on S, then S is subdirectly irreducible.

Proof. Let N be the least nondegenerate ideal of S. By corollary 4.24, N induces a proper congruence ρ on S defined by

$$x_\rho = \begin{cases} N \text{ for each } x \in N \\ \{x\} \text{ for each } x \in S\setminus N. \end{cases}$$

If γ is any proper congruence on S, then 0_γ is a nondegenerate ideal of S by hypothesis, and so $N \subseteq 0_\gamma$. If $(a,b) \in \rho\setminus\varepsilon_S$, then $a \neq b$, and so $\{a\} \neq \{b\}$. Since $a_\rho = b_\rho$, then $a_\rho \neq \{a\}$ and $b_\rho \neq \{b\}$, so that $a_\rho = b_\rho = N$. Hence $a \in N \subseteq 0_\gamma$ and

$b \in N \subseteq 0_\gamma$, so that $a_\gamma = b_\gamma = 0_\gamma$, and thus $(a,b) \in \gamma$. Therefore, if $(a,b) \in \rho \setminus \varepsilon_s$, then $(a,b) \in \gamma$, so that $\rho \setminus \varepsilon_s \subseteq \gamma$. Since $\varepsilon_s \subseteq \gamma$ as well, then $\rho = \varepsilon_s \cup (\rho \setminus \varepsilon_s) \subseteq \gamma$. Thus ρ is the least proper congruence on S, and so S is subdirectly irreducible.

It so happens that the converse of theorem 4.25 is false. This is a consequence of the fact that the converse of corollary 4.24 is false, as shown by the following example.

Example 4.26. Let $S = \{0,1,2\}$ be the semigroup of integers modulo 3 with modular multiplication. Define ρ on S by $1_\rho = 2_\rho = \{1,2\}$; $0_\rho = \{0\}$. Then ρ is the least proper congruence on S, and so S is subdirectly irreducible. However, although ρ is a proper congruence on S, $0_\rho = \{0\}$ is a degenerate ideal of S. However, the following somewhat weaker result is true.

Theorem 4.27. Let S be a subdirectly irreducible semigroup with zero 0. If 0_ρ is a nondegenerate ideal of S whenever ρ is a proper congruence on S, then there exists a least nondegenerate ideal of S.

Proof. Since S is subdirectly irreducible, then there exists a least proper congruence ρ on S. By hypothesis, 0_ρ is a nondegenerate ideal of S. If N is any nondegenerate ideal of S, then $0 \in N$. By corollary 4.24, N induces a proper congruence γ on S defined by

$$x_\gamma = \begin{cases} N & \text{for each } x \in N \\ \{x\} & \text{for each } x \in S \setminus N, \end{cases}$$

and so $\rho \subseteq \gamma$. Therefore, if $a \in 0_\rho$, then $(a,0) \in \rho \subseteq \gamma$, so that $a_\gamma = 0_\gamma = N$ since $0 \in N$, and thus $a \in N$. Hence $0_\rho \subseteq N$, and so 0_ρ is the least nondegenerate ideal of S.

Corollary 4.28. If S is a semigroup with zero 0 in which 0_ρ is a nondegenerate ideal of S whenever ρ is a proper congruence on S, then S is subdirectly irreducible iff S has a least nondegenerate ideal.

Proof. Suppose S has a least nondegenerate ideal. Since 0_ρ is a nondegenerate ideal of S whenever ρ is a proper congruence on S, then the hypothesis of theorem 4.25 is satisfied, and so S is subdirectly irreducible.

Conversely, suppose S is subdirectly irreducible. Since 0_ρ is a nondegenerate ideal of S whenever ρ is a proper congruence on S, it follows that S has a least nondegenerate ideal by theorem 4.27.

CHAPTER BIBLIOGRAPHY

1. Petrich, Mario, Introduction to Semigroups, Columbus, Ohio, Charles E. Merrill Publishing Company, 1973.

BIBLIOGRAPHY

1. Petrich, Mario, Introduction to Semigroups, Columbus, Ohio, Charles E. Merrill Publishing Company, 1973.

2. Shapiro, Louis, Introduction to Abstract Algebra, New York, McGraw-Hill Book Company, Inc., 1975.