IDEMPOTENT SEMIGROUPS WITH DISTRIBUTIVE RIGHT CONGRUENCE LATTICES

R. A. DEAN AND ROBERT H. OEHMKE

A great deal of effort in the study of semigroups has been spent in an attempt to adopt group theoretic methods to semigroups and to find suitable analogues for group concepts that will be significant in the general structure theory of semigroups. Of particular importance in the study of groups are the various relationships between a group and its subgroups. As is well-known each subgroup in a group induces a decomposition of the group into right cosets. In turn, this decomposition corresponds to an equivalence relation that is invariant under right multiplication. We call such an equivalence relation a right congruence. Since there is a one-to-one correspondence between the set of right congruences of a group and the set of subgroups of the group it is clear that any subgroup-group relationship can be translated into one involving these right congruences.

In semigroup theory the importance of the subsemigroup structure to the nature of the semigroup is not quite so clear. This is due primarily to the fact that there is very little relationship between the homomorphisms of a semigroup and the subsemigroups of the semigroup. Thus in studying lattices associated with semigroups we have chosen to study the right congruences of a semigroup rather than the more obvious analogue of subgroup, the subsemigroup, studied by Ego, et al, [3, 7, 8].

In § 1 we show that these right congruences form a complete lattice which is compactly generated in the sense of Crawley and Dilworth [2, p. 2]. It is natural to ask what are the implications for the semigroup of restraints which may be placed on this related lattice.

As a first problem in this area we seek a characterization of those semigroups whose lattice of right congruences is distributive. For groups this answer was determined by Ore [6, Theorem 4] to be the locally cyclic groups. It is shown in § 2 that the lattice of right congruences of a locally cyclic semigroup is distributive. (It should be noted here that Severin [7] has shown that the lattice of semigroups of a locally cyclic semigroup is not necessarily distributive.) However, as is seen, not all semigroups with distributive right congruence lattices need be locally cyclic. Thus the characterization problem remains. While we have no solution to this problem in general, we do give in §§ 3 and 4 necessary and sufficient conditions for an idempotent semigroup to have a distributive lattice of right congruences. § 3 treats

Received August 13, 1963.

commutative idempotent semigroups (semi-lattices) and § 4 treats arbitrary idempotent semigroups. In § 5 a necessary and sufficient condition for an idempotent semigroup to have both its lattice of right congruences and its lattice of left congruences distributive is given. Finally in § 6 idempotent semigroups with a distributive lattice of right congruences are characterized in terms of simpler structures.

1. Let τ be an equivalence relation on a semigroup S. We shall write either $a\tau b$ or $a \equiv b \pmod{\tau}$ if the ordered pair (a, b) belongs to the relation τ.

An equivalence relation τ on a semigroup S is a *right* (*left*) *congruence* if $a, b, c \in S$ and $a\tau b$ implies $ac\tau bc$ ($ca\tau cb$).

In this section we denote by $\mathfrak{L}_r(S)$ the set of all right congruences on the semigroup S. We shall use Latin letters to denote elements of S and Greek letters to denote elements of $\mathfrak{L}_r(S)$. $\mathfrak{L}_r(S)$ is never empty since the relation ι defined by $a\iota b$ if and only if $a = b$ is trivially a right congruence as is the universal relation υ in which $a\upsilon b$ holds for all elements of S. We impose the natural ordering on $\mathfrak{L}_r(S)$; namely, that $\alpha \leqq \beta$ if and only if $a\alpha b$ implies $a\beta b$ for all a, b in S. It is easy to see that if Γ is any set of right congruences then $\cap \Gamma$ defined by $a \equiv b \pmod{\cap \Gamma}$ if and only if $a\gamma b$ for all $\gamma \in \Gamma$ is a right congruence on S, and is the greatest lower bound of Γ in $\mathfrak{L}_r(S)$ under the partial ordering $\leqq$. This, together with the fact that ν is a maximal element in $\mathfrak{L}_r(S)$ guarantees that $\mathfrak{L}_r(S)$ is a complete lattice under $\leqq$.

It is important to obtain a better characterization of the least upper bound $\cup \Gamma$ of a set Γ of right congruences. As is customary in such matters we have the following result whose proof we omit.

LEMMA 1. *Let $a, b \in S$, and let Γ be a set of right congruences on S. $a \equiv b \pmod{\cup \Gamma}$ if and only if there is a finite sequence $a = x_1, x_2, \cdots, x_n = b$ of elements in S and a sequence $\gamma_1, \cdots, \gamma_{n-1}$ in Γ such that $x_i\gamma_i x_{i+1}$ for $i = 1, \cdots, n-1$.*

As a consequence of this lemma and of the definition of $\cup \Gamma$ it follows easily that $\mathfrak{L}_r(S)$ is a sublattice of the lattice $\mathfrak{P}(s)$ of all partitions on S considered as an abstract set.

To prove that $\mathfrak{L}_r(S)$ is compactly generated we need to identify the minimal congruence $\tau_{a,b}$ identifying a with b. We have of course that $\tau_{a,b} = \cap \{\gamma \mid a\gamma b\}$. Of interest is the alternate description afforded by the next lemma.

LEMMA 2. *Let ρ be any partition of S. Define ρ' by $a\rho' b$ if and only if either $a\rho b$ or there are elements r, s, t in S such that $a = rt$, $b = st$ and $r\rho s$. If σ is the transitive closure of ρ', then σ*

is the smallest equivalent relation in $\mathfrak{P}(s)$ *which is a right congruence ccontaining* ρ, *hence in* $\mathfrak{L}_r(S)$, $\sigma = \cap\{\alpha \in \mathfrak{L}_r(S) \mid a\rho b \Rightarrow a\alpha b\}$.

Proof. A straightforward calculation shows that σ is a right congruence containing ρ. Thus it remains to show that if τ is a right congruence containing ρ it must also contain σ. Certainly if $a\rho' b$ then $a\tau b$ since τ is a right congruence and so $r\tau s$ implies $(rt)\tau(st)$. From this it follows easily that if $a\sigma b$ then $a\tau b$ and thus $\sigma \leqq \tau$.

This lemma gives the characterization of $\tau_{a,b}$ by taking ρ to be the partition which identifies a, b and no other distinct pair of elements of S. The σ of the lemma is then $\tau_{a,b}$.

THEOREM 1. $\mathfrak{L}_r(S)$ *is a complete, compactly generated lattice.*

Proof. We have already proved completeness. It is clear that if $\alpha \in \mathfrak{L}_r(S)$ then $\alpha = \cup\{\gamma_{a,b} \mid a\alpha b\}$ and so it remains only to show that for each pair of elements $\tau_{a,b}$ is a compact element of $\mathfrak{L}_r(S)$. Suppose that $\tau_{a,b} \leqq \cup \Gamma$ where Γ is any set of right congruences on S. In particular we have that $a \equiv b \pmod{\cup \Gamma}$ and by Lemma 1 there are sequences $a = x_1, \cdots, x_n = b$ and $\gamma_1, \cdots, \gamma_{n-1}$ such that $x_i\gamma_1 x_{i+1}$. Thus $a \equiv b \bmod (\gamma_1 \cup \gamma_2 \cup \cdots \cup \gamma_n)$ and by Lemma 2 therefore $\tau_{a,b} \leqq \gamma_1 \cup \cdots \cup \gamma_n$.

Another type of right congruence construction which we frequently employ is the following. Suppose that I is a right ideal of S. Let $\tau = \tau(I)$ be defined by $a\tau b$ if and only if $a = b$ or a and b are both members of I. τ is easily seen to be a right congruence which, following Clifford and Preston [1, p. 17], we call the Rees right congruence defined by I.

THEOREM 2. *If S is a semigroup having three mutually disjoint right ideals I_1, I_2, I_3 then $\mathfrak{L}_r(S)$ is not distributive.*

Proof. Clearly the set union of I_2 and I_3, denoted by $I_2 \cup I_3$, is a right ideal. We let $\tau_1 = \tau(I_1) \cup \tau(I_2 \cup I_3)$ and define τ_2 and τ_3 as cyclic variants. Because $I_i \cap I_j = \varphi$ it follows that $\tau_i \cap \tau_j = \tau(I_1) \cup \tau(I_2) \cup \tau(I_3)$ while $\tau_i \cup \tau_j = \tau(I_1 \cup I_2 \cup I_3)$ and so $\tau_1 \cap (\tau_2 \cup \tau_3) \neq (\tau_1 \cap \tau_2) \cup (\tau_1 \cap \tau_3)$.

2. LEMMA 3. *Let S be an arbitrary semigroup, τ and σ be right congruences on S and $x \in S$. Then*

(1) $A(\tau, x) = \{n \colon x^i \tau x^j$ *and* $n = i - j\}$ *is an ideal in the ring of integers. If* $A(\tau, x) = (d)$ *we write* $\alpha(\tau, x) = d$;

(2) *if* $(0) \neq A(\tau, x) = d$, *then there is a unique positive integer* $\mu(\tau, x) = r$ *such that* $x^r \tau x^{r+d}$ *and if* $x^a \tau x^s$ *with* $1 \leqq a < r$ *then* $a = s$;

(3) *for all* $x \in S$, $A(\sigma \cap \tau, x) = \text{l.c.m.}\ (\alpha(\sigma, x), \alpha(\tau, x))$ *and* $\mu(\sigma \cap \tau, x) = \max(\mu(\sigma, x), \mu(\tau, x))$;

(4) *if S is the cyclic semiqroup $\langle x \rangle$ then* $\alpha(\sigma \cup \tau, x) =$ g.c.d. $(\alpha(\sigma, x), \alpha(\tau, x))$ *and* $\mu(\sigma \cup \tau, x) = \min(\mu(\sigma, x), \mu(\tau, x))$.

Proof. To prove (1), suppose that n and $m \in A(\tau, x)$, say $x^i\tau x^{i+n}$ and $x^j\tau x^{j+m}$. Hence $x^{i+j}\tau x^{i+j+n}$ and $x^{i+j}\tau x^{i+j+m}$ so that $x^{i+j+n}\tau x^{i+j+m}$. Thus $n - m \in A(\tau, x)$ and so $A(\tau, x)$ is an ideal.

To prove (2), choose $\mu(\tau, x)$ to be the least positive integer r such that $x^r\tau x^{r+d}$. Now suppose $x^a\tau x^s$ with $1 \leqq a < r$ and $a \neq s$. Without loss of generality we may assume $a < s$. Then we may conclude $x^{r-1}\tau x^t$ where $t = s + (r - a) - 1$ and $r - 1 < t$. Now $d \mid (r - 1) - t$ so that $t = (r - 1) + kd = r + kd - 1 = r + (d - 1) + (k - 1)d$ with $k \geqq 1$. From $x^r\tau x^{r+d}$ we conclude $x^r\tau x^{r+(k-1)d}$. Therefore $x^{r+(d-1)}\tau x^{r+(d-1)+(k-1)d}$ and $x^{r-1+d}\tau x^t$. But $x^t\tau x^{r-1}$ and so $x^{r-1}\tau x^{(r-1)+d}$, contrary to the choice of r.

In the proof of (3) and (4) we may suppose $A(\tau, x) \neq (0) \neq A(\sigma, x)$ since if $A(\tau, x) = (0)$ then clearly $A(\sigma \cap \tau, x) = A(\sigma \cup \tau, x) = A(\sigma, x)$. We let $A(\tau, x) = (p)$, $\mu(\tau, x) = r$, $A(\sigma, x) = (q)$, and $\mu(\sigma, x) = s$. Assume $r \leqq s$.

To prove (3) let $m =$ l.c.m. (p, q) with $m = pp_1 = qq_1$. We have $x^r\tau x^{r+p}\tau x^{r+pp_1}$ and so $x^s\tau x^{s+m}$. Similarly $x^s\sigma x^{s+m}$ so that $m \in A(\sigma \cap \tau, x)$. Let $A(\sigma \cap \tau, x) = m_1$ and $\mu(\sigma \cap \tau, x) = t$. *Thus* $x^t(\sigma \cap \tau)x^{t+m_1}$ and in particular $x^t\sigma x^{t+m_1}$ so that $p \mid m_1$ and similarly $q \mid m_1$. Hence $m \mid m_1$ and since $m \in (m_1)$, we have $m = m_1$. From $x^s(\sigma \cap \tau)x^{s+m}$ it follows that $\mu(\sigma \cap \tau, x) \leqq s$. On the other hand from $x^t(\sigma \cap \tau)x^{t+m}$ it follows that $x^t\sigma x^{t+m}$. Now (2) implies that either $m = 0$ or $s \leqq t$.

To prove (4) let $d =$ g.c.d. (p, q). There is a solution w for the congruence $wp \equiv d \pmod q$ with w arbitrarily large. Indeed, if we choose v so that $r + d + vp > s$ then we may find a solution w so that for $u = w + v$ we have $r + up > s$. With these choices we have $(u - v)p \equiv d \pmod q$ and $x^r\tau x^{r+up}$ and $x^{r+up}\sigma x^{r+d+vp}$ since $q \mid d + vp - up$ and $r + up > s$. But $x^{r+d+vp}\tau x^{r+d}$ and so $x^r(\sigma \cup \tau)x^{r+d}$. This shows that $d \in A(\sigma \cup \tau, x)$.

Now let $t = \mu(\sigma \cup \tau, x)$ and $(e) = A(\sigma \cup \tau, x)$. Thus $e \mid d$. From $x^t(\sigma \cup \tau)x^{t+e}$ we know there are integers $t = a_0, a_1, \cdots, a_n = t + e$ so that $x^{a_i}\delta x^{a_{i+1}}$ where $\delta = \sigma$ or τ and where $a_i \neq a_{i+1}$. For each i we have either that $p \mid a_{i+1} - a_i$ or $q \mid a_{i+1} - a_i$ and so for all i we have $d \mid a_{i+1} - a_i$. Hence $d \mid \Sigma_i (a_{i+1} - a_i)$ or $d \mid a_n - a_0 = e$. Hence $d = e$ and since $x^r(\sigma \cup \tau)x^{r+d}$ it follows that $\mu(\sigma \cup \tau, x) = t \leqq r \leqq s$. Now consider $x^t\delta x^{a_1}$. Since $t \neq a_1$ it follows from (2) that $t \geqq r$ if $\delta = \tau$ and $t \geqq s \geqq r$ if $\delta = \sigma$. In either event, $t \geqq r$. Hence $t = r$ and the lemma is proved.

From this lemma the following theorem is easily established.

THEOREM 3. *If S is a locally cyclic semigroup then its lattice of right congruences is distributive.* (The word "right" is superfluous since a locally cyclic semigroup is abelian.)

Proof. Let ρ, σ, τ be congruences on S. We are to show $\rho \cap (\sigma \cup \tau) = (\rho \cap \sigma) \cup (\rho \cap \tau)$. To simplify notation let $\phi = \rho \cap (\sigma \cup \tau)$ and $\theta = (\rho \cap \sigma) \cup (\rho \cap \tau)$. As in any lattice $\phi \supseteqq \theta$ so we need only show $\phi \subseteqq \theta$. Let $a\phi b$. Then $a\rho b$, $a(\sigma \cup \tau)b$ and there is a sequence $a = a_1, \cdots, a_n = b$ with $a_i \delta a_{i+1}$ and $\delta = \sigma$ or τ. Since S is locally cyclic there is a c with $a = c^e$, $b = c^f$ and $a_i \in < c >$. Hence we can assume $S = < c >$. By Lemma 3

$$\begin{aligned}\alpha(\phi, c) &= \text{l.c.m.}\,(\alpha(\rho, c), \text{g.c.d.}\,(\alpha(\sigma, c), \alpha(\tau, c)))\\ &= \text{g.c.d.}\,(\text{l.c.m.}\,(\alpha(\rho, c), \alpha(\sigma, c))), \text{l.c.m.}\,(\alpha(\rho, c), \alpha(\tau, c)))\\ &= \alpha(\theta, c)\,,\\ \mu(\phi, c) &= \max\,(\mu(\rho, c), \min\,(\mu(\sigma, c), \mu(\tau, c)))\\ &= \min\,(\max\,(\mu(\rho, c), \mu(\sigma, c)), \max\,(\mu(\rho, c), \mu(\tau, c)))\\ &= (\mu(\theta, c)\,.\end{aligned}$$

Let $\alpha(\phi, c) = \alpha(\theta, c) = d$ and $\mu(\phi, c) = \mu(\theta, c) = r$ and $e = f$. Then either $e = f$ or $r \leqq e < f$ and $d \mid f - e$. Hence from $c^e \phi c^f$ we easily get $c^e \theta c^f$.

COROLLARY. *If S is an infinite cyclic semigroup then its congruence lattice is the direct product of a countably infinite chain and the lattice of integers partially ordered by division. If S is a finite cyclic semigroup, $\{a, a^2, \cdots, a^r, a^{r+1}, \cdots, a^{r+m} = a^r\}$ then its congruence lattice is the direct product of a chain of length r and the divisor lattice of m.*

Proof. It is easily verified that if S is a cyclic semigroup with generator a, the mapping $\phi \to (\mu(\phi, a), \alpha(\phi, a))$ is a one-to-one mapping of the congruence lattice onto the direct product of the lattices mentioned in the corollary. It is also easy to see that $\phi \leqq \theta$ in the congruence if and only if $\mu(\phi, a) \geqq \mu(\theta, a)$ and $\alpha(\theta, a) \mid \alpha(\phi, a)$, so that the correspondence is a lattice isomorphism. Note that the ordering of the chain *reverses* the "natural" ordering.

3. A *semilattice* is a commutative idempotent semigroup S. If we define

$$(1) \qquad a \leqq b \text{ if and only if } ba = a$$

then S is partially ordered by this relation and $ab = a \cap b =$ greatest lower bound of a and b.

Let S be a semilattice. Whenever $a \geqq b$ we let $a/b = \{x \mid a \geqq x \geqq b\}$ which we call the *quotient* a over b. We say that a/b *projects down* to c/d if $a \geqq c \geqq d \geqq bc$. We write $a/b \to c/d$.

LEMMA 4. *In the semilattice S, the following properties hold:*
(i) $a/b \to c/d$ *implies* $a/b \to cx/dx$ *for all* $x \in S$;
(ii) $a/b \to c/d$ *and* $c \geqq e \geqq f \geqq d$ *imply* $a/b \to e/f$;
(iii) $a/b \to c/d$ *and* $a/b \to d/e$ *imply* $a/b \to c/e$;
(iv) $a/b \to c/d$ *and* $c/d \to e/f$ *imply* $a/b \to e/f$.

Proof.
(i) We have $a \geqq c \geqq d \geqq bc$. From $c \geqq d \geqq bc$ we conclude $c \geqq cx \geqq dx \geqq (bc)x \geqq b(cx)$.

(ii) We have $a \geqq c \geqq e \geqq f \geqq d \geqq bc$. From $c \geqq e$ we conclude $bc \geqq be$ while from $e \geqq bc$ we conclude $be \geqq b(bc) = bc$. Hence $bc = be$ and $a \geqq e \geqq f \geqq be$.

(iii) We have $a \geqq c \geqq d \geqq bc$ and $a \geqq d \geqq e \geqq bd$. From $d \geqq bc$ we have $bd \geqq b(bc) = bc$ and thus $a \geqq c \geqq e \geqq bd \geqq bc$. Thus $a/b \to c/e$.

(iv) We have $a \geqq c \geqq d \geqq bc$ and $c \geqq e \geqq f \geqq de$. From $d \geqq bc$ we have $de \geqq (bc)e = b(ce)$. Now $c \geqq e$ implies $e = ce$, hence $de \geqq be$. Thus $a \geqq e \geqq f \geqq be$, that is $a/b \to e/f$.

THEOREM 4. *Let S be a semilattice. Let $a \geqq b$ in S. The minimal congruence identifying a and b, $\tau_{a,b} = \tau$, is characterized by*

$$x\tau y \text{ if and only if } x = y \text{ or } a/b \to x/xy \text{ and } a/b \to y/xy .$$

Proof. For brevity let us write $x \sim y$ if $x = y$ or if $a/b \to x/xy$ and $a/b \to y/xy$. The relation $(\sim)$ is clearly reflexive and symmetric.

First we establish that $x \sim y$ implies $x\tau y$. We suppose that $a/b \to x/xy$ and $a/b \to y/xy$. We shall show that $x\tau xy$ and, by symmetry, $y\tau xy$; whence $x\tau y$ follows. Now $a/b \to x/xy$ means $a \geqq x \geqq xy \geqq bx$. $a \geqq x$ implies $ax = x$ and so $axy = xy$ and $x \geqq xy \geqq bx$ implies $bx \geqq bxy \geqq bx$, hence $bx = bxy$. On the other hand $a\tau b$ implies $ax\tau bx$ and $axy\tau bxy$; in other words $x\tau bx$ and $xy\tau bx$. Thus $x\tau xy$.

We next show that $(\sim)$ is a congruence relation on S and $a \sim b$. This completes the proof, since the above paragraph then shows that $(\sim) \leqq \tau$ while $\tau \leqq (\sim)$ by the minimal nature of τ.

(i) $a \sim b$ holds by the definition of a projection since $ab = b$.

(ii) $x \sim y$ implies $xz \sim yz$ since if $a/b \to x/xy$, then $a/b \to xz/xyz$ by property (i) of Lemma 3.

(iii) To show that $(\sim)$ is transitive suppose that $x \sim y$ and $y \sim z$. If $x = y$ or $y = z$ then clearly $x \sim z$. Thus we suppose that $a/b \to x/xy$, $a/b \to y/xy$, $a/b \to y/yz$, and $a/b \to z/yz$. By property (i) we have $a/b \to xy/xyz$ and thus by property (iii) $a/b \to x/xyz$. Finally, since $x \geqq xz \geqq (xz)y = xyz$ it follows from property (ii) that $a/b \to x/xz$. By symmetry $a/b \to z/xz$ and thus $x \sim z$.

COROLLARY. *With the notation of the theorem, $a\tau x$ if and only* *if* $a \geqq x \geqq b$.

Proof. If $a \geqq x \geqq b$ then $ax = x$, $bx = b$ and $ax\tau bx$ implies $x\tau b$ and hence $a\tau x$. Conversely, $a\tau x$ implies $a/b \rightarrow a/xa$ and $a/b \rightarrow x/xa$; hence $a \geqq a \geqq xa \geqq ba = b$, $a \geqq x \geqq xa \geqq bx$ and $a \geqq x \geqq b$.

THEOREMS. *In a semilattice S, for any two elements a, b it is true that* $\tau_{a,b} = \tau_{a,ab} \cup \tau_{b,ab}$.

Proof. $a(\tau_{a,ab} \cup \tau_{b,ab})b$ since $a\tau_{a,ab}ab\tau_{b,ab}b$. Hence $\tau_{a,b} \leqq \tau_{a,ab} \cup \tau_{b,ab}$. On the other hand for any congruence τ, $a\tau b$ implies $a\tau ab$ and $ab\tau b$. Thus in particular $\tau_{a,b} \geqq \tau_{a,ab}$ and $\tau_{a,b} \geqq \tau_{b,ab}$ which implies $\tau_{a,b} \geqq \tau_{a,ab} \cup \tau_{b,ab}$.

For semilattices we need the concepts of an ideal and a dual ideal. A subset I of a semi-lattice is called an *ideal*, if when $a \in I$ and $x \leqq a$ then $x \in I$. It is clear that this is but a reformulation of an ideal in a semigroup in the special case when the semigroup is a semilattice. A *dual ideal* is a subset J such that if (i) $a \in J$ and $a \leqq x$ then $x \in J$ and (ii) if $a \in J$ and $b \in J$ then $ab \in J$.

THEOREM 6. *Let S be a semilattice containing three distinct elements a, b, c such that b and c are noncomparable but such that* $a > b$ *and* $a > c$. *Then the lattice of congruences on S is nonmodular.*

Proof. Let $\rho = \tau_{b,bc}$, $\sigma = \tau_{a,b}$ and $\tau = \tau_{a,c}$. Clearly $\rho \leqq \tau$ as $a/c \rightarrow b/bc$ and so $b\tau bc$. We shall prove that while $\rho \leqq \tau$ it is false that $\tau \cap (\rho \cup \sigma) = \rho \cup (\sigma \cap \tau)$.

First note that since $a > b$ and $a > c$ while b and c are noncomparable, the corollary to Theorem 4 implies that $a \not\equiv c \pmod{\sigma}$.

Second note that $a/b \rightarrow c/bc$ and so $c\sigma bc$. Thus we have $c\sigma bc$, $bc\rho b$, and $b\sigma a$; that is, $c(\rho \cup \sigma)a$. Thus $\tau \leqq \rho \cup \sigma$ and $\tau \cap (\rho \cup \sigma) = \tau$. It now suffices to show that $a \not\equiv c \bmod \rho \cup (\sigma \cap \tau)$.

To simplify matters we replace ρ by a possibly larger congruence φ. φ is the Rees congruence generated by the ideal $I = \{x: x \leqq b\}$. Since $b\varphi bc$ it follows that $\rho \leqq \varphi$. We claim in fact that $a \not\equiv c \bmod (\varphi \cup (\sigma \cap \tau))$.

Note that $x\varphi y$ and $x > b$ imply $x = y$ and in particular that $a\varphi x$ implies $a = x$. Also, from the corollary if $a\sigma x$ and $a\tau x$ then $a \geqq x \geqq b$ and $a \geqq x \geqq c$. Suppose, then, that there is a sequence

$$a = x_1, x_2, \cdots, x_n = c \qquad (n > 2)$$

so that $x_i\varphi x_{i+1}$ or $x_i(\sigma \cap \tau)x_{i+1}$. Without loss of generality we suppose that we have selected a sequence of minimal length. Now if $a = x_1\varphi x_2$, then $x_2 = a$ and x_2 could have been deleted from the sequence. Thus $a = x_1(\sigma \cap \tau)x_2$ and $a \geqq x_2 \geqq b$. In fact, since $a \not\equiv b \pmod{\tau}$ we have $x_2 > b$. Now if $n \geqq 3$, and if $x_2(\sigma \cap \tau)x_3$, then $x_1(\sigma \cap \tau)x_3$ and x_2 could have been deleted. Thus if $n \geqq 3$, it must be that $x_2 \varphi x_3$. But $x_2 > b$ and hence $x_3 = x_2$ so that x_3 could have been deleted from the sequence. Thus it must be that $n = 2$ and that $a(\sigma \cap \tau)c$; the latter is a contradiction since $a \not\equiv c \pmod{\sigma}$.

THEOREM 7. *Let S be a semilattice. A congruence τ is uniquely determined by the set of quotients a/b such that $a\tau b$. That is if $Q(\tau) = \{a/b \mid a\tau b\}$ then $Q(\tau) = Q(\sigma)$ implies $\sigma = \tau$. Moreover $\sigma \leqq \tau$ if and only if $Q(\sigma) \subseteqq Q(\tau)$.*

Proof. It clearly suffices to prove the last conclusion of the theorem. If $\sigma \leqq \tau$ then $Q(\sigma) \subseteqq Q(\tau)$ holds trivially. Suppose then that $Q(\sigma) \subseteqq Q(\tau)$ and that $x\sigma y$. Thus $x\sigma xy$ and $xy\sigma y$. Thus x/xy and $y/xy \in Q(\sigma) \subseteqq Q(\tau)$. Thus $x\tau xy$ and $xy\tau y$, whence $x\tau y$, and consequently $\sigma \leqq \tau$.

THEOREM 8. *Let S be a semilattice in which elements with a common upper bound are comparable* i.e., *for all $a, b, c \in S$, if $a \geqq b$ and $a \geqq c$ then either $b \geqq c$ or $c \geqq b$. The lattice of congruence relations on S form a distributive lattice.*

Proof. Let ρ, σ, τ be three elements of $\mathfrak{L}_r(S)$. We are to show that $\rho \cap (\sigma \cup \tau) = (\rho \cap \sigma) \cup (\rho \cap \tau)$. Since $\rho \cap (\sigma \cup \tau) \geqq (\rho \cap \sigma) \cup (\rho \cup \tau)$ in any lattice we need only establish the reverse relation and in view of Theorem 7 we need only show that $Q[\rho \cap (\sigma \cup \tau)] \subseteqq Q[(\rho \cap \sigma) \cup (\rho \cap \tau)]$.

We shall first prove that under the conditions of the theorem if $a/b \in Q(\sigma \cup \tau)$ then there is a sequence $a = x_1 \geqq x_2 \geqq \cdots \geqq x_n = b$ so that for each i, $x_i/x_{i+1} \in Q(\sigma) \cup Q(\tau)$. Now if $a/b \in Q(\sigma \cup \tau)$ we have $a(\sigma \cup \tau)b$ so that there is a sequence $a = y_1, y_2, \cdots, y_n = b$ with $y_i \alpha_i y_{i+1}$ where $\alpha_i = \sigma$ or τ. From this sequence we construct the desired sequence by setting $x_i = y_1 y_2 \cdots y_i$. Clearly $x_i \geqq x_{i+1}$ and $x_i = y_1 \cdots y_i \alpha_i y_1 \cdots y_i y_{i+1}$ so that $x_i/x_{i+1} \in Q(\sigma) \cup Q(\tau)$. Since $a \geqq x_i$ and $a \geqq b = y_m \geqq x_m$, from the hypothesis it must be the case that x_i and b are comparable, for all i. If we choose n as the least integer such that $b \geqq x_n$, then we may conclude that $a = x_1 \geqq \cdots \geqq x_{n-1} > b$ and thus $x_1, \cdots, x_{n-1}, b$ is the desired chain.

Now suppose that $c/d \in Q[\rho \cap (\sigma \cup \tau)]$. Then $c\rho d$ and $c/d \in Q(\sigma \cup \tau)$. By the preceeding paragraph there is a chain $c = x_1 \geqq x_2 \geqq \cdots \geqq x_n = d$ with $x_i/x_{i+1} \in Q(\sigma) \cup Q(\tau)$. Since $c\rho d$ it follows from the Corollary to Theorem 4 that $x_i \rho x_{i+1}$ and thus $x_i(\rho \cap \sigma)x_{i+1}$ or $x_i(\rho \cap \tau)x_{i+1}$; in any event $c \equiv d \bmod (\rho \cap \sigma) \cup (\rho \cap \tau)$.

We may now combine Theorems 6 and 8 to obtain an answer to our question in the case of semilattices.

COROLLARY. *A semilattice has a distributive lattice of congruences if and only if every pair of elements with a common upper bound are comparable.*

4. We define a relation R on the idempotent semigroup S by aRb if and only if

$$ab = b \quad \text{and} \quad ba = a$$

and a relation L by aLb if and only if

$$ab = a \quad \text{and} \quad ba = b .$$

It has been shown by McLean [5, Lemma 4] that both R and L are equivalence relations. In fact R is a left congruence and L is a right congruence [5, Lemma 5]. We shall denote the equivalence class of a under R and L respectively by R_a and L_a.

Further, if W is the relation defined by aWb if and only if

$$aba = a \quad \text{and} \quad bab = b$$

then W is a two-sided congruence (homomorphism) on S, the homomorphic image of S under W is a semilattice $\mathfrak{W}$ [5, Theorem 1] and W_a, the equivalence class of a under W, is the direct product of L_a and R_a [4, Lemma 1] and $W_a = L_aR_a$.

We shall use the notations $W_a \circ W_b$ for the multiplication in $\mathfrak{W}$ and $W_a W_b$ for ordinary complex multiplication. Also, we shall use the notation $W_a \leqq W_b$ for the ordering defined in (1) on the semilattice $\mathfrak{W}$.

We prove the following elementary consequences of these results:

(2) $W_x \circ W_a = W_a \circ W_x = W_{xa} = W_{ax}$.

(3) $W_{xy} \leqq W_x$ and $W_{xy} \leqq W_y$.

(4) $W_a \leqq W_b$ implies $W_a \circ W_b = W_a$ and $W_b W_a \cup W_a W_b \subseteqq W_a$.

(5) $R_a \subseteqq W_a$ and $L_a \subseteqq W_a$.

(6) If $W_y = R_y$ and $W_y \leqq W_a$ then $ay = y$.

(7) If $W_y = L_y$ and $W_y \leqq W_a$ then $ya = y$.

The first three of these were obtained by McLean [5]. From $W_a = L_aR_a$, $aR_a = R_a$ and $L_a a = L_a$ it follows that (5) holds. If $W_y = R_y$ and $W_y \leqq W_a$ then $W_{ay} = W_y$ and $ay \in W_y = R_y$. Therefore $y(ay)y = y$. But $y(ay) = ay$ and we have (6). We prove (7) in a similar manner.

THEOREM 9. *If S is an idempotent semigroup such that the lattice $\mathfrak{L}_r(S)$ is modular then for all $y \in S$ either $L_y = \{y\}$ or $R_y = \{y\}$.*

Proof. Assume $z \in L_y$ and $z \neq y$. We shall consider three basic right congruences, τ_1, τ_2 and L. L was defined above. τ_1 shall be the right congruence whose only possible nontrivial equivalence classes are R_y and the ideal $I = \{x \mid W_x < W_y\}$. τ_2 shall have only R_z and I as its possible nontrivial equivalence classes.

First we prove that τ_1 and (by symmetry) τ_2 are right congruences. Set $a\tau_1 b$. We are to show $ac\tau_1 bc$ for all $c \in S$. We have $W_{ac} \leqq W_a$ and $W_{bc} \leqq W_b$. Thus if $a, b \in I$ then $ac, bc \in I$ and thus $ac\tau_1 bc$. If $a, b \in R_y$ then $a, b \in W_y$ and $W_{ac} = W_{bc}$. If $W_{ac} \leqq W_y$ then ac and hence $bc \in I$ so that $ac\tau_1 bc$. If $W_{ac} = W_y = W_{bc}$ then $ac, bc \in R_y$ since W is an equivalence relation. Hence $ac\tau_1 bc$.

Now, to complete the proof of the theorem, let $x \in R_y$. We will show $x = y$. We use the fact that modularity implies

$$(\tau_1 \cup \tau_2) \cap (\tau_2 \cup L) = \tau_2 \cup [(\tau_1 \cup \tau_2) \cap L] .$$

By the definition of τ_1 we have $x\tau_1 y$ and hence $x(\tau_1 \cup \tau_2)y$. Next we show $x(\tau_2 \cup L)y$. First we note yLz and hence $yxLzx$. Since $x \in R_y$, $yx = x$, so that $xLzx$. Now $zx \in R_z$ since $z(zx) = zx$ and $(zx)z = z$ by the definition of W_y. Therefore $zx\tau_2 zx$. We now have

$$xLzx;\ zx\tau_2 z;\ zLy$$

and

$$x(L \cup \tau_2)y .$$

In summary $x \equiv y \bmod (\tau_1 \cup \tau_2) \cap (\tau_2 \cup L)$ and by modularity $x \equiv y \bmod \tau_2 \cup [(\tau_1 \cup \tau_2) \cap L]$. However both x and y are in trivial equivalence classes of τ_2. If $y \equiv a \bmod ((\tau_1 \cup \tau_2) \cap L)$ then yLa and $y(\tau_1 \cup \tau_2)a$. Thus we have $a \in L_y$. But $R_z \cap R_y = \varphi$ for if $b \in R_z \cap R_y$ then $zb = b$, $by = y$ and $(zb)y = by = y$. However, $z(by) = zy = z$. It follows that the only possible nontrivial equivalence classes of $\tau_1 \cup \tau_2$ are R_y, R_z and I. Hence $a \in R_y$. We now have $a \in R_y \cap L_y = \{y\}$. Thus y lies in a trivial equivalence class under both τ_2 and $(\tau_1 \cup \tau_2) \cap L$ and hence under $\tau_2 \cup [(\tau_1 \cup \tau_2) \cap L]$. Therefore $y = x$ and $R_y = \{y\}$.

THEOREM 10. *Let S be an idempotent semigroup. $\mathfrak{L}_r(S)$ is distributive if and only if*

(i) *$\mathfrak{L}(\mathfrak{W})$ is distributive.*

(ii) *For all $a \in S$, W_a contains at most two elements.*

(iii) *If $W_a = L_a \neq \{a\}$ then W_a is the smallest element of $\mathfrak{W}$.*

(iv) *If $W_x < W_y$ then either $W_x W_y = \{xy\}$ or $W_x = L_x$.*

Proof. We first assume $\mathfrak{L}_r(S)$ is distributive. If σ is a right congruence of $\mathfrak{W}$ define σ' by

$$a\sigma' b \qquad \text{if and only if} \qquad W_a \sigma W_b .$$

A straightforward proof shows that the correspondence $\sigma \to \sigma'$ is a lattice isomorphism of $\mathfrak{L}(\mathfrak{W})$ into $\mathfrak{L}_r(S)$. Hence $\mathfrak{L}(\mathfrak{W})$ is distributive.

By Theorem 9, $W_y = L_y$ or R_y.

In order to prove that (iii) is necessary for $\mathfrak{L}_r(S)$ to be distributive we assume y is an element of S such that $L_y = W_y \neq \{y\}$. Now let T be a subset of L_y and I the right ideal defined by

$$I = \{x \mid W_x < W_y\} .$$

If $a \in S$ and $z \in L_y$ then by (3), $W_{za} \leqq W_z = L_y$. If $W_{za} = W_z$ then $W_z \leqq W_a$ and by (7) we have $za = z$. This says that if T is any subset of L_y then either

$$(8) \qquad Ta \subseteqq I \quad \text{or} \quad Ta = T .$$

Now let $\mathfrak{T}$ be any decomposition of L_y into disjoint subsets and let ρ be the equivalence relation defined by

$$a\rho b \text{ if and only if } a = b \text{ or } a, b \in I \text{ or } a, b \in T \text{ for some } T \in \mathfrak{T} .$$

It follows from (8) that ρ is a right congruence. Now let $T_0 \in \mathfrak{T}$ and define an equivalence relation ρ' by

$$a\rho' b \text{ if and only if } a = b \text{ or } a, b \in T_0 \cup I \text{ or } a, b \in T \text{ for some } T \in \mathfrak{T} .$$

Again it follows from (8) that ρ' is a right congruence.

Now let $y \neq z \in L_y$ and τ_1, τ_2 and τ_3 be the right congruences whose only possible nontrivial equivalence classes are

$$\tau_1 : \{y\} \cup I$$
$$\tau_2 : \{z\} \cup I$$
$$\tau_3 : \{z, y\}, I .$$

The only possible nontrivial equivalence class of either $\tau_1 \cap \tau_2$ or $\tau_1 \cap \tau_3$ is I. Therefore if $a \in I$ then

$$y \not\equiv a \,(\mathrm{mod}\,(\tau_1 \cap \tau_2) \cup (\tau_1 \cap \tau_3)) .$$

However $\tau_1 \leqq \tau_2 \cup \tau_3$ and $a\tau_1 y$. Therefore

$$a \equiv y \,(\mathrm{mod}\,\tau_1 \cap (\tau_2 \cup \tau_3))$$

and

$$\tau_1 \cap (\tau_2 \cap \tau_3) \neq (\tau_1 \cap \tau_2) \cup (\tau_1 \cap \tau_3) .$$

Hence if $\mathfrak{L}_r(S)$ is distributive then we must assume I is empty and thus (iii) holds.

In the same way, if w is an element of L_y distinct from y and z

we can show that the right congruences τ_1, τ_2, τ_3 whose nontrivial equivalence classes are

$$\tau_1 : \{y, z\}$$
$$\tau_2 : \{y, w\}$$
$$\tau_3 : \{w, z\}$$

fail to satisfy the distributive law. Therefore (ii) holds for all $W_y = L_y$.

To prove (ii) in the case $W_y = R_y$ we shall proceed as in the case $W_y = L_y$. However, to establish the necessary right congruence properties we need a weak form of (iv); namely, if $R_y < W_a$ then $R_y a = \{ya\}$. Assume $R_y < W_a$ and there is a pair x, x' in R_y such that

$$xa \neq x'a .$$

We let $xa = y$ and $x'a = y'$. Then $ya = y$ and $y'a = y'$. Let σ_y and $\sigma_{y'}$ be the right congruences defined by

$$c\sigma_y b \text{ if and only if } yc = yb$$
$$c\sigma_{y'} b \text{ if and only if } y'c = y'b .$$

We have

$$a\sigma_y y \quad \text{and} \quad a\sigma_{y'} y' .$$

Therefore

$$y \equiv y' \pmod{\sigma_y \cup \sigma_{y'}} .$$

Thus if $\tau_{y,y'}$ is the minimal right congruence relating y and y' we must have

$$\tau_{y,y'} \leqq \sigma_y \cup \sigma_{y'}$$

and

$$y \equiv y' \pmod{\tau_{y,y'} \cap (\sigma_y \cup \sigma_{y'})} .$$

Now let $z \in R_y$ and $z \equiv z' \pmod{\tau_{y,y'} \cap \sigma_y}$. Since $z\sigma_y z'$ we have $yz' = yz = z$ and $R_y = R_{yz} = W_{yz'} \leqq W_{z'}$. But we also have

$$z\tau_{y,y'}z' . \tag{9}$$

Let τ be the right congruence corresponding to the right ideal

$$J = \{x \mid W_x \leqq R_y\} .$$

Since $y\tau y'$ we have $\tau_{y,y'} \leqq \tau$. Therefore from $z \in R_y$ and (9) we have $z' \in J$ and $W_{z'} \leqq R_y$. Thus $W_{z'} = R_y$ and $z' = yz' = yz = z$. We can now conclude that if $z \in R_y$ then z is in a trivial equivalence class of

$$(\tau_{y,y'} \cap \sigma_{y'}) \cup (\tau_{y,y'} \cap \sigma_y) .$$

To avoid a contradiction to the assumption that $\mathfrak{L}_r(S)$ is distributive we must assume that if $W_a \geqq R_y$ then $y'a = ya$ for all $y' \in R_y$ or

$$R_y a = \{ya\} .$$

We now have sufficient multiplicative properties for R_y to show, just as in the case $W_y = L_y$, that if $\mathfrak{T}$ is any decomposition of R_y then the collection $\mathfrak{T} \cup \{I\}$, $I = \{x : W_x < R_y\}$, can be extended in a trivial way to a decomposition of S and the corresponding relation is a right congruence. This follows chiefly from the fact proved above that if $T \subseteqq R_y$ then either T_a is a single element of R_y or $Ta \subseteqq I$. If x, y, z are distinct elements of R_y then the three right congruences τ_1, τ_2, τ_3 corresponding to the decompositions of R_y:

$$\tau_1 : \{x, y\} ,$$
$$\tau_2 : \{y, z\} ,$$
$$\tau_3 : \{x, z\} ,$$

do not satisfy the distributive law since

$$x \equiv y \ (\mathrm{mod}\ \tau_1 \cap (\tau_2 \cup \tau_3))$$

and

$$x \not\equiv y \ (\mathrm{mod}\ (\tau_1 \cap \tau_2) \cup (\tau_1 \cap \tau_3)) .$$

Therefore R_y contains at most two elements.

We can now prove a slightly stronger result on the multiplicative properties of the R_y's and thus prove (iv). Assume $R_y = \{y, z\}$ and $W_a > R_y$. If $W_a = \{a\}$ then from the above results we have $R_y W_a = R_y a = \{ya\}$. We shall show that the same result holds if $W_a = \{a, b\}$. Since $W_a > R_y$ we cannot have $W_a = L_a$. Hence we must have $W_a = R_a$. Let ρ and δ be the right congruences defined by

$$c\rho d \text{ if and only if } W_c = W_d \leqq R_a$$
$$c\delta d \text{ if and only if } W_c = W_d < R_a .$$

If $\mathfrak{L}_r(S)$ is distributive then since $\delta \leqq \rho$ we have

$$\rho \cap (\sigma_y \cup \delta) = (\rho \cap \sigma_y) \cup \delta \tag{10}$$

where σ_y was defined above. Assume $R_y a = \{y\}$. Then $ya = y^2$ and $y \equiv a \ (\mathrm{mod}\ \sigma_y)$. Multiplying by b we have $yb \equiv ab \ (\mathrm{mod}\ \sigma_y)$ and $yb \equiv b \ (\mathrm{mod}\ \sigma_y)$. Therefore

$$a\sigma_y y;\ y\delta yb;\ yb\sigma_y b$$

and

$$a \equiv b \, (\text{mod}\, \sigma_y \cup \delta)$$
$$a \equiv b \, (\text{mod}\, \rho \cap (\sigma_y \cup \delta)) \, .$$

On the other hand, by (10), there is a minimal sequence $a = x_1, \cdots, x_n = b$ such that $x_i \alpha_i x_{i+1}$ where α_i is either $\rho \cap \sigma_y$ or δ. Since a is in a trivial equivalence class of δ and the sequence $x_1, \cdots, x_n$ is minimal we have $a \neq x_2$ and $a \equiv x_2 \, (\text{mod}\, \rho \cap \sigma_y)$. Therefore $a \rho x_2$. But $x_2 \in R_a$; thus $x_2 = b$, $a \equiv b \, (\text{mod}\, \rho \cap \sigma_y)$ and $a \equiv b \, (\text{mod}\, \sigma_y)$. Therefore $ya = yb$ and $R_y R_a = \{ya\}$.

We now prove the sufficiency of the four conditions of the theorem. Since each W_a contains at most two elements we must have either $W_a = R_a$ or $W_a = L_a$.

LEMMA 5. *If $R_a = \{a, b\}$ and σ is a right congruence such that $a \sigma x$ for $x \neq a$ then $a \sigma b$.*

Proof. Since $ab = b$ and $a \sigma x$ we have

$$a \sigma (xa)$$

and

$$b \sigma (xb) \, .$$

Also, $W_{xb} = W_{xa}$. If W_{xb} is a singleton then $xb = xa$ and $a \sigma b$. If $W_{xb} = R_{xb} \leqq W_b$ then $xa \in W_{xb}$ and (iv) implies $(xa)a = (xa)b$ and $xa = xb$. Thus $a \sigma b$.

If $W_{xb} = L_{xb}$ then $(xb)a = xb$ by (7). But $(xb)a = x(ba) = xa$. Then $xb = xa$ and again $a \sigma b$.

LEMMA 6. *If $a \equiv b$ $(\text{mod}\, \sigma \cup W)$ then either*

(1) *$a \sigma b$,*

(2) *$a W b$, or*

(3) *there exist distinct elements y and z such that $az = y$, $by = z$, $L_y = \{y, z\}$ and $a \sigma y W z \sigma b$.*

Proof. Assume there is a minimal sequence $x_1, \cdots, x_n$ such that $a = x_1$, $b = x_n$ and $x_i \alpha_i x_{i+1}$ where $\alpha_i = \sigma$ or W. If all α_i are equal then, by transitivity either $a \sigma b$ or $a W b$. Also since the sequence of x's is minimal we can assume $\alpha_i \neq \alpha_{i+1}$. Therefore for some i we have either $x_{i-1} \sigma x_i W x_{i+1}$ or $x_{i-1} W x_i \sigma x_{i+1}$; say the first of these holds. By Lemma 5, if $W_{x_i} = R_{x_i}$ then $x_{i-1} \sigma x_{i+1}$. But then the minimality of the sequence is contradicted. Therefore we can assume that each $x_i \neq a, b$ must be in $W_y = L_y = \{y, z\}$. If $i > 4$ then either y or z is duplicated in the sequence, and hence it could be shortened. Therefore we must have either

$$a\,Wx_2\sigma x_3\,Wb$$

or

$$a\sigma x_2\,Wx_3\sigma b\ .$$

If the first of these alternatives hold we have $a, b \in L_y$, since $x_2, x_3 \in L_y$, and $W_a = W_b$. So assume the second alternative holds. Then

$$ax_3\sigma x_2x_3 = x_2 \quad\text{and}\quad x_3 = x_3x_2\sigma bx_2\ .$$

If either $ax_3 = x_3$ or $bx_2 = x_2$ then $x_3\sigma x_2$ and $a\sigma x_2\,Wx_3\sigma b$ implies $a\sigma b$ and the lemma is proved.

LEMMA 7. *If* $az = y$, $by = z$, $L_y = \{y, z\}$, $y \neq z$ *and* $a\sigma b$ *then* a, b, y *and* z *are congruent under* σ.

Proof. Let $c \in S$ such that $W_c = R_c$. If $cz = y$ then $cy = c^2z = cz = y$. If $d \in R_c$ then $d = cd$ and $dz = cdz = c(dz) = y$ since $dz \in L_y$. Therefore $R_cL_y = \{y\}$. In the same way if $cy = z$ we have $R_cL_y = \{z\}$. Now $bab, aba \in W_{ab}$. Thus, if $W_{ab} = R_{ab}$ then $babz = abaz$. But by a direct calculation $b(abz) = z$ and $a(baz) = y$. Hence $W_{ab} \neq R_{ab}$ and indeed bab and aba are distinct. Since $babz \neq abaz$ we must have $W_{ab} = L_y$; i.e., $ab, ba \in L_y$. From $abz = y$ and $bay = z$ and the definition of L_y we have $ab = y$ and $ba = z$. We can now conclude that $a\sigma b$ implies $a^2\sigma ba$, $ab\sigma b^2$ and consequently $a\sigma z$ and $y\sigma b$.

For any right congruence δ we define δ' as $\delta' = \delta \cup W$. It is clear that δ' is a right congruence on $\mathfrak{W}$ and $\delta_1' \cup \delta_2' = (\delta_1 \cup \delta_2)'$. In addition we have

LEMMA 8. $(\delta_1' \cap \delta_2') = (\delta_1 \cap \delta_2)'$.

Proof. It follows readily from the definition of δ_i' and lattice-theoretical properties that

$$\delta_1' \cap \delta_2' \geqq (\delta_1 \cap \delta_2)'\ ;$$

therefore we assume

$$a \equiv b \bmod \delta_1' \cap \delta_2'$$

and show

$$a \equiv b \bmod (\delta_1 \cap \delta_2)'\ . \tag{11}$$

Since $a \equiv b \bmod \delta_1'$ we can conclude that for each i; (1), (2) or (3) of Lemma 6 holds. If the same case holds for both δ_i then clearly (11) is satisfied. Again (11) is satisfied if for either δ_i (2) holds. This leaves a mixed case, say $a\delta_1 b$ and $a\delta_2 y Wz \delta_2 b$ where $az = y$, and $by = z$. Applying Lemma 7 we have $a\delta_1 y$, $z\delta_1 b$ and $a\delta_1 y Wz\delta_1 b$. Therefore $a(\delta_1 \cap \delta_2)y Wz(\delta_1 \cap \delta_2)b$ and the proof is complete.

To prove the distributivity of $\mathfrak{L}_r(S)$ we consider three right congruences τ_1, τ_2 and τ_3. By lattice-theoretical properties we have

$$\tau_1 \cap (\tau_2 \cup \tau_3) \geqq (\tau_1 \cap \tau_2) \cup (\tau_1 \cap \tau_3) .$$

So assume

$$a \equiv b \,(\mathrm{mod}\, \tau_1 \cap (\tau_2 \cup \tau_3)) . \tag{12}$$

If $W_a = W_b$ and $a \neq b$ then from (12) we have $a(\tau_2 \cup \tau_3)b$ and therefore there is an $x \neq a$ such that either $a\tau_2 x$ or $a\tau_3 x$. If $W_a = W_b = R_a$ then by Lemma 5 we have either $a\tau_2 b$ or $a\tau_3 b$. In either case $a \equiv b \bmod (\tau_1 \cap \tau_2) \cup (\tau_1 \cap \tau_3)$. If $W_a = W_b = L_y = \{y, z\}$ then $y \equiv z \,(\mathrm{mod}\, \tau_2 \cup \tau_3)$ and there is a sequence $y = x_1, \cdots, x_n = z$ such that

$$x_i \alpha_i x_{i+1}$$

for all $i = 1, \cdots, n$ and $\alpha_i = \tau_2$ or τ_3. Multiplying by y, we have $x_i y \alpha_i x_{i+1} y$. Since $x_1 y = y$, $x_n y = z$ and $x_i y$ is either y or z there must be an i such that $y\alpha_i z$. Hence either $a\tau_2 b$ or $a\tau_3 b$ and

$$a \equiv b \bmod (\tau_1 \cap \tau_2) \cup (\tau_1 \cap \tau_3) . \tag{13}$$

It remains to show (13) holds when $W_a \neq W_b$. From (12) we have

$$a \equiv b \bmod \tau_1' \cap (\tau_2' \cup \tau_3') .$$

By the distributivity of $\mathfrak{L}(\mathfrak{W})$ we then have

$$a \equiv b \bmod (\tau_1' \cap \tau_2') \cup (\tau_1' \cap \tau_3') .$$

But, by Lemma 8,

$$(\tau_1' \cap \tau_2') \cup (\tau_1' \cap \tau_3') = (\tau_1 \cap \tau_2)' \cup (\tau_1 \cap \tau_3)' = [(\tau_1 \cap \tau_2) \cup (\tau_1 \cap \tau_3)]' = \sigma'$$

and either (13) holds or (3) of Lemma 6 holds. However if (3) holds then from (12) and Lemma 7 a, b, y, z are related by $\tau_1 \cap (\tau_2 \cup \tau_3)$. Since $W_y = W_z = L_y$ then by the argument above $y \equiv z \bmod \sigma$. Also, from Lemma 6, we have

$$a\sigma y Wz\sigma b .$$

Therefore $a\sigma y$; $y\sigma z$; $z\sigma b$ and $a\sigma b$. Hence (13) holds in all cases and

$$\tau_1 \cap (\tau_2 \cup \tau_3) = (\tau_1 \cap \tau_2) \cup (\tau_1 \cap \tau_3) .$$

Thus $\mathfrak{L}_r(S)$ is distributive.

5. We now let $\mathfrak{L}_r(S)$ be the lattice of right congruences of S and $\mathfrak{L}_l(S)$ be the lattice of left congruences of S we have

THEOREM 11. *Let S be an idempotent semigroup. Then $\mathfrak{L}_r(S)$ and $\mathfrak{L}_l(S)$ are distributive if and only if S is a distributive semilattice or S is the union of two nonempty distributive semilattices Z_x and Z_y with zeros x and y respectively such that if $a \in Z_x$ and $b \in Z_y$ then*

(1) $ab = x$ *and* $ba = y$

or

(2) $ab = y$ *and* $ba = x$.

Proof. We first assume $\mathfrak{L}_r(S)$ and $\mathfrak{L}_l(S)$ are distributive. While the results of the preceding theorem and proof were obtained for $\mathfrak{L}_r(S)$ it can be seen that the dual results hold for $\mathfrak{L}_l(S)$. Thus for example since any nontrivial L_y must satisfy $L_y \leqq W_a$ for all a we have, by duality, that any nontrivial R_y must satisfy $R_y \leqq W_a$ for all a. Hence if there is any nontrivial W_y we must have $W_y \leqq W_a$ for all a.

We now prove one further result for a nontrivial $R_y = \{y, x\}$ using the distributivity of $\mathfrak{L}_r(S)$. We let

$$Z_y = \{a \mid ya = y\} = \{a \mid xa = y\}$$
$$Z_x = \{a \mid xa = x\} = \{a \mid ya = x\} .$$

Since $R_y a = \{ya\} \in R_y$ we have $Z_y \cap Z_x = \phi$. If $W_a > R_y$, $ya = y$ and $b \in W_a$ then $yb = y$ since $R_y W_a = \{ya\}$, i.e., if $a \in Z_y$, $b \in W_a$ and $W_a > R_y$ then $b \in Z_y$. Similarly if $a \in Z_x$, $b \in W_a$ and $W_a > R_y$ then $b \in Z_x$. Let $a \in Z_x$, $b \in X_y$ then

$$y(ab) = (ya)b = xb = x .$$

Therefore $ab \in Z_y$. In this manner we show that both Z_y and Z_x are left ideals of S. Then $aba \in Z_x$. But $aba \in W_{ab}$ and $ab \in Z_y$. Therefore if $W_{ab} > R_y$ we have $aba \in Z_y$ and $aba \in Z_x \cap Z_y$. Hence we must have $W_{ab} = R_y$. Since the only element of R_y in Z_y is y we have $ab = y$. Similarly $ba = x$.

Since $R_y = \{y, x\}$ must satisfy $R_y \leqq W_a$ for all a we have $S = Z_y \cup Z_x$. Also, since there is only one nontrivial W_a then Z_y and Z_x must be semilattices.

Again using the duality principle, if $L_y = \{y, x\}$ then there are two disjoint semilattices Z_x and Z_y such that x is a zero of Z_x, y is a zero of Z_y and $a \in Z_x$ and $b \in Z_y$ implies

$$ab = x \quad \text{and} \quad ba = y .$$

In this case let σ be a right congruence of S. Let σ_x and σ_y be the right congruences induced by σ on Z_x and Z_y respectively. Also let δ be the congruence whose only nontrivial equivalence class is L_y.

Now, since Z_x is a right ideal any (right) congruence τ on Z_x may be extended to a (right) congruence τ' on S by defining $a\tau' b$ if and only if $a = b$ or $a, b \in Z_x$ and $a\tau b$. In this way we extend σ_x and σ_y to congruences σ'_x and σ'_y.

We claim that $\sigma = \sigma'$ where

$$\sigma' = \sigma'_x \cup \sigma'_y \qquad \text{if} \quad x \not\equiv y \bmod \sigma$$
$$\sigma' = \sigma'_x \cup \sigma'_y \cup \delta \quad \text{if} \quad x \equiv y \bmod \sigma \,.$$

We note that if $a\sigma b$ with $a \in Z_x$, $b \in Z_y$ then $a\sigma ba$, or $a\sigma y$ and $ab\sigma b$ or $x\sigma b$; hence $x\sigma y$. Thus $\sigma \geqq \sigma'$. Conversely, suppose $a\sigma b$. If $\{a, b\} \subseteqq Z_x$ or Z_y then clearly $a\sigma' b$. If for example $a \in Z_x$ and $b \in Z_y$ then, as above, $a\sigma y\sigma x\sigma b$, so that $a\sigma'_y y\delta x\sigma' b$, and we have $a\sigma' b$. It now follows that

$$\mathfrak{L}_r(S) = \mathfrak{L}_r(Z_x) \times \mathfrak{L}_r(Z_y) \times \{\iota, \delta\} \,.$$

Note that since Z_x and Z_y are semilattices then the congruences of $\mathfrak{L}_r(Z_x)$ and $\mathfrak{L}_r(Z_y)$ are two sided. Also both L and δ are two sided. Therefore $\mathfrak{L}_l(S) = \mathfrak{L}_r(S)$.

Using the duality once more we can concluded that we have the same result if $R_y = \{y, x\}$.

We have just shown that if $S = Z_x \cup Z_y$ with Z_x and Z_y defined as in the statement of the theorem then

$$\mathfrak{L}_r(S) = \mathfrak{L}(Z_x) \times \mathfrak{L}(Z_y) \times \{\iota, \delta\} \,.$$

Since $\{\iota, \delta\}$ is a distributive lattice then a necessary and sufficient condition that $\mathfrak{L}_r(S)$ be distributive is that both $\mathfrak{L}(Z_x)$ and $\mathfrak{L}(Z_y)$ be distributive. This concludes the proof of the theorem.

The following corollary is a consequence of one of the remarks made in the above proof.

COROLLARY. *If $\mathfrak{L}_r(S)$ and $\mathfrak{L}_l(S)$ are both distributive then every congruence of S is two-sided.*

6. In this section we give a more detailed description of an idempotent semigroup S whose right congruence lattice is distributive. Throughout this section we shall consider a semigroup satisfying conditions (i), (ii), (iii), and (iv) of Theorem 10. We denote by y and z the unique pair (if they exist) of elements such that $W_y = L_y = \{y, z\}$.

DEFINITION. For $a \in S$ let $S_a = \{b \mid W_{ab} \neq L_y\}$.

In particular S_y is empty and if no y and z exist, $S_a = S$. Also, if $W_a \neq W_y$ then $a \in S_a$ so that $S_a \neq \phi$.

LEMMA 9. *If* $W_a \geqq W_b \neq W_y = L_y$ *then* $S_a = S_b$. *In particular if* $x \in S_a$, $S_a = S_{ax} = S_x$.

Proof. Now $W_a \geqq W_b$ implies $W_{ax} \geqq W_{bx}$ for all $x \in S$. Thus if $W_{bx} \neq L_y$, then $W_{ax} \neq L_y$ and so $S_b \subseteqq S_a$. On the other hand, suppose that $x \in S_a$. Since $W_a \geqq W_{ax}$ and $W_a \geqq W_b$ from condition (i) we must have that $W_{ax} \geqq W_b$ or $W_b \geqq W_{ax}$. Hence $W_{ax} \circ W_b = W_{axb}$ is either W_b or W_{ax}, neither of which is W_y. But $W_{bx} \geqq W_{axb}$ and so $W_{bx} \neq W_y$. Thus $x \in S_b$ so that $S_a \subseteqq S_b$.

As an immediate consequence we have that if $x \in S_a$, then $S_a = S_{ax} = S_x$.

LEMMA 10. *For all* $a, b, \in S$, *either* $S_a \cap S_b = \varphi$ *or* $S_a = S_b$.

Proof. If $S_a \cap S_b \neq \varphi$, let $c \in S_a \cap S_b$. From Lemma 9, $S_a = S_{ac} = S_c$ while $S_b = S_{bc} = S_c$.

LEMMA 11. *If* S_a *is nonempty,* S_a *is a sub-semigroup of* S *and* $S_a \cup W_y$ *is a two-sided ideal.*

Proof. Let $b, c \in S_a$. From Lemma 9 we have $S_a = S_b = S_{bc}$; in particular $bc \in S_a$. The fact that $S_a \cup W_y$ is a two-sided ideal follows easily from the observation that for all $x \in S$, $W_a \geqq W_{ax} = W_{xa} \geqq W_y$.

LEMMA 12. *If* $a, b \notin L_y$ *and* $W_a \circ W_b = L_y$ *then* $aS_b = \{ab\}$.

Proof. Let b and $b' \in S_b$. Thus $W_{bb'} \neq L_y$ and so $W_{bb'} = R_{bb'}$. By (6) we then have, since $W_b > W_{bb'}$, that $b(b'b) = b'b$. Again, since ab and $ab' \in L_y$, and $W_{b'b} > W_y$ it follows from (7) that $ab = ab(b'b)$ and $(ab')b'b = (ab')b = ab'$. Thus $ab = abb'b = ab'b = ab'$.

LEMMA 13. *Let* $a \notin L_y$. *If* $x \in S_a$ *and* $xz = xy$ *then* $uy = uz = xz$ *whenever* $u \in S_a$ *and* $W_u \leqq W_x$.

Proof. Without loss of generality suppose $xy = xz = y$. Now $W_u \leqq W_x$ and $W_u = R_u$ so that $xu = u$. Also the hypothesis implies $uxz = uy$.

If $ux = u$, then $uz = uy$ and it must follow that $uz = uy = y$ for if it were the case that $uz = uy = z$ then $y = xz = x(uz) = (xu)z = uz = z$; a contradiction. Thus we may suppose that $W_u = R_u = \{u, u'\}$ and that $ux = u'$, hence that $ux = u'x = u'$. On the other hand since $u'x = u'$ we may replace u by u' in the above argument to conclude $u'y = u'z = y$ and so $uu'y = uy$. But $uu' = u'$ so that $uy = y$. Similarly if $uz = z$ it follows that $u'uz = u'z$, or $uz = u'z = z$, a contradiction. In this way we have $y = uy = uz$.

LEMMA 14. *Let $a \notin L_y$. If $az = y$ then for $x \in S_a$, $xy = y$.*

Proof. We have $az = ay = y$. Let $x \in S_a$. If $W_x \leqq W_a$ the result is that of Lemma 13. On the other hand if $W_x \geqq W_a$ and $xy = z$ then from Lemma 13 it would follow that $az = ay = z$, a contradiction. Hence $xy = y$ in this case. Finally suppose that W_x and W_a are incomparable. We have $W_a > W_{ax}$ By Lemma 13 $axz = axy = y$. Also $W_x > W_{ax}$ and if $xy = z$, then Lemma 13 gives $axy = z$, a contradiction. Thus $xy = y$.

COROLLARY. *Let $a \notin L_y$. Either $xy = y$ for all $x \in S_a$ or $xz = z$ for all $x \in S_a$.*

Proof. If $bz = y$ for some $b \in S_a = S_b$, then, from Lemma 14, $xy = y$ for all $x \in S_b = S_a$.

LEMMA 15. *In S, the following two alternatives obtain:*

(1) *For all $a \notin L_y$, $ay = az$.*

(2) *There exists a vnique S_a such that for some $a_0 \in S_a$ it is true that $a_0y = y$ and $a_0z = z$. Moreover if $W_{a_1} \geqq W_{a_0}$, then $a_1y = y$ and $a_1z = z$.*

Proof. Suppose that (1) does not hold. Then for $a_0 \notin L_y$, $a_0y = y$ and $a_0z = z$. (If $a_0y = z$, then $a_0y = a_0z = z$.) Now if $b \notin S_{a_0}$ then $ba_0 \in L_y$ and so

$$(ba_0)y = ba_0 = b(a_0y) = by$$

and

$$(ba_0)z = ba_0 = b(a_0z) = bz$$

so that $by = bz$. Thus it follows that if $ay = y$ and $az = z$ it must be the case that $a \in S_{a_0}$. This establishes the uniqueness of S_{a_0}.

Now suppose that $W_a \geqq W_{a_0}$. If $ay = az$ then Lemma 13 shows that $a_0y = a_0z$, a contradiction. Hence $ay = y$ and $az = z$.

COROLLARY. *The set $D = \{W_a \mid ay = y \text{ and } az = z\}$ forms a dual ideal of $\mathfrak{W}$.*

Proof. First note that from condition (2) of Lemma 15, D is well defined, and indeed if $W_a \in D$ and $W_{a_1} \geqq W_a$ then $W_{a_1} \in D$. Lastly, if

$W_a \in D$ and $W_b \in D$ then $W_a \circ W_b = W_{ab} \in D$ since from $ay = by = y$ and $az = bz = z$ it follows that $aby = y$ and $abz = z$.

LEMMA 16. *If $a \notin L_y$ and $ay = az$ then for $b \notin S_a$, $ab = ay = az$. Moreover, if $xy = xz$ for all $x \in S_a$ then if $S_b \neq S_a$, $S_aS_b = \{ay\}$. Finally if $a \notin L_y$ and $ay = y$, $az = z$ then for $b \notin S_a$, $ab = by$.*

Proof. Since $b \notin S_a$, $ab \in L_y$ and so $ab = a(ab) = ay = az$. Under the second assumption $xy = xz = ay = az$ and so $xb = ab = ay = az$, for all $x \in S_a$. On the other hand, from Lemma 12, $aS_b = \{ab\}$, thus $S_aS_b = \{ab\} = \{ay\}$. Under the third assumption we have $ab \in W_y$, $ab = aby = by$ since $by \in W_y$.

As a result of Lemmas 10 and 11 we may write S as the disjoint union of sub-semigroups S_a and the sub-semigroup $W_y = L_y = \{y, z\}$. Lemmas 12–16 describe how these semigroups multiply. The typical possibilities are summarized in the table below. We assume that

(14) S_a contains an element a_0 such that $a_0y = y$ and $a_0z = z$ and other elements x such that $xy = xz$;

(15) that $S_b \neq S_a$ and $by = bz = y$, and

(16) $S_c \neq S_a$ and $cy = cz = z$. A single entry in a box means that all entries in that box have the entered value.

	S_a		S_b	S_c	$\cdots$	y	z
S_a	a_0	$\cdots$ S_a	y	z	$\cdots$	y	z
	x	$\cdots$	xy	xy	xy	$xy = xz$	
S_b		y	S_b	y	y	y	y
S_c		z	z	S_c	z	z	z
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
y		y	y	y	y	y	y
z		z	z	z	z	z	z

Another way of decomposing S is to construct

$$I_y = \{x \mid xy = xz = y\}$$
$$I_z = \{x \mid xy = xz = z\}$$

and

$$J = \{x \mid xy = y, xz = z\} .$$

It is easy to see that these sets are mutually disjoint and that I_y and I_z are left ideals. It is clear that if J is nonempty it contains those elements of the single set S_a such that $by = y$ and $bz = z$. Any other S_x falls into either I_y or I_z. The remainder (if any) of the S_a falls into either I_y or I_z depending on whether $by = y$ or $bz = z$ for all $b \in S_a$.

Idempotent semigroups whose right congruence lattices are distributive may be constructed by pasting together semigroups with the structure of an S_a by using the rules laid down in Lemma 9–16. Thus let $\mathfrak{S}$ be a collection of distinct semigroups S_a satisfying conditions (i), (ii), (iv), and in addition that $W_x = R_x$ for all x. Let y and z be elements not appearing in $\cup \mathfrak{S}$. $\cup \mathfrak{S} \cup \{y, z\}$ is made into a semigroup by defining the multiplication between the sets S_a and $\{y, z\}$. It is convenient to think of this as being done in a multiplication table. We insist that $yx = y$, $zx = z$, for all x. For all S_b, with one possible exception we may choose with complete freedom, we define for $x \in S_b$, $xy = xz \in \{y, z\}$. The choice of the particular value is arbitrary. Then for all $c \notin S_b$, xc is defined to be $xy = xz$. For $c \in S_b$, the multiplication is of course to be that of S_b. After this stage only the exceptional semigroup, call it S_a, has yet to be handled. In $\mathfrak{W}(S_a)$ let D be any dual ideal. We define $dy = y$, $dz = z$ if $W_d \in D$. For all $x \notin D$ we make $xy = xz \in \{y, z\}$ and the choice is again arbitrary. We now claim that under these rules $\cup \mathfrak{S} \cup \{y, z\}$ is an idempotent semigroup with distributive right congruence lattice.

To verify that the associative law holds we need to check several cases of the identity $p(qr) \equiv (pq)r$.

Case 1. $S_p = S_q = S_r$ or $\{p, q, r\} \leqq \{y, z\}$. Here p, q, r belong to a set assumed to be a sub-semigroup.

Case 2. $p \in \{y, z\}$. Here the multiplication gives $(pq)r = pr = p = p(qr)$.

Hereafter we assume that $p \notin \{y, z\}$.

Case 3. $py = pz$. By Lemma 16, $px = py = pz$ for all $x \notin S_p$ so that associativity holds here.

Case 4. $py = y$ and $pz = z$. Thus $p \in S_a$ and in $\mathfrak{W}(S_a)$, $W_p \in D$. In view of the corollary to Lemma 14 we may suppose, without loss of generality, that for all $x \in S_a$ such that $W_x \notin D$, $xy = xz = y$.

If $q \in \{y, z\}$ then $p(qr) = pq = q$ while $(pq)r = qr = q$, and so we may assume $q \notin \{y, z\}$. We may also suppose that $qr \notin S_a$, otherwise $S_p = S_q = S_r$. Under these assumptions for Case 4 two main subcases arise.

Case 4.1. $S_q = S_r \neq S_a$. From Lemma 13 we have $pq = pr = p(qr)$ and since $pq \in \{y, z\}$ we have $(pq)r = pq$. Thus associativity holds.

Case 4.2. $S_q \neq S_r$. Here $qr \in \{y, z\}$ so that under the hypothesis of Case 4, $p(qr) = qr$. If $S_p \neq S_q$, then from Lemma 16 we have $pq = qy = qz = qr$, so that $(pq)r = (qr)r = qr$. Thus in this case we may assume $S_p = S_q = S_a \neq S_r$, in particular we have $pq \in S_p = S_a$. Now if $W_{pq} \in D$, then since $W_q \geqq W_{pq}$ we have $W_q \in D$ and thus $qy = y$ and $qz = z$. Since $S_r \neq S_q$ it follows that $ry = rz$ and thus from Lemma 16, that $qr = ry = rz = (pq)r$. On the other hand, if $W_{pq} \notin D$ it follows that, since $W_p \in D$, it must be the case that $W_q \notin D$. Thus $(pq)r = y$ and $qr = y$ from the Case 4 assumptions; so that $p(qr) = py = y$. This completes the verification of the associative law.

Finally we need to see that conditions (i), (ii), (iii) and (iv) of Theorem 10 are satisfied. From the multiplication table it is easily seen that for all $x \in \bigcup \mathfrak{S}$, W_x is unchanged in the large semigroup while $W_y = L_y = \{y, z\} = L_z = W_z$ is the minimal element of $\mathfrak{W}$. Thus conditions (ii) and (iii) hold. $\mathfrak{L}(\mathfrak{W})$ is distributive since for the large semigroup, $\mathfrak{W}$ is the set sum of the individual $\mathfrak{W}_a$ of the member semigroups together with W_y. The only new order relations present are $W_y < W_x$ for all $x \in \bigcup \mathfrak{S}$. For this reason it is clear that (iv) holds since if $L_a \neq W_a < W_b$ it must be that $S_a = S_b$ and condition (iv) was assumed to hold in S_a.

BIBLIOGRAPHY

1. A. H. Clifford, and G. B. Preston, *The Algebraic theory of semigroups, Volume* 1 Amer. Math. Soc., (1961).
2. R. P. Dilworth and Peter Crawley, *Decomposition theory for lattices without chain conditions,* Trans. Amer. Math. Soc., **96** (1960), 1-22.
3. M. Ego, *Structures des demi-groupes dont le treillis des sous-demi-groups satisfait à certaines conditions,* Bull. Soc. Math. France **91**, (1963), 138-201.
4. N. Kimura, *The structure of idempotent semigroups,* Pacific J. Math., **8** (1958), 257-275.
5. D. McLean, *Idempotent semigroups,* Amer. Math. Mon., **61** (1954), 110-113.
6. O. Ore, *Structures and group theory,* Duke Math. J., **21** (1938), 247-269.
7. L. N. Sevrin, *Semigroups with certain types of sub-semigroup lattices,* Dokl. Akad. Nauk. S.S.S.R., **138** (1961), 796-798.
8. Takayuki Tamura, *Semigroups and their subsemigroup lattices,* Pacific J. Math., **13** (1963), 725-736.

CALIFORNIA INSTITUTE OF TECHNOLOGY
INSTITUTE FOR DEFENSE ANALYSIS