3-1950

Prime Ideals in Semigroups

Helen Bradley Grimble
University of Tennessee - Knoxville

To the Graduate Council:

I am submitting herewith a thesis written by Helen Bradley Grimble entitled "Prime Ideals in Semigroups." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Arts, with a major in Mathematics.

D. D. Wilson, Major Professor

We have read this thesis and recommend its acceptance:

Wallace Givens, O. G. Harrold Jr. Walter S. Snyder

Accepted for the Council:
Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

March 9, 1950

To the Committee on Graduate Study:

I am submitting to you a thesis written by Helen Bradley Grimble entitled "Prime Ideals in Semi-groups." I recommend that it be accepted for nine quarter hours of credit in partial fulfillment of the requirements for the degree of Master of Arts, with a major in Mathematics.

D. D. Miller
Major Professor

We have read this thesis
and recommend its acceptance:

Wallace Givens

O. N. Harrold, Jr.

Walter S. Snyder

Accepted for the Committee

E. G. Waters
Dean of the Graduate School

PRIME IDEALS IN SEMIGROUPS

A THESIS

Submitted to
The Committee on Graduate Study
of
The University of Tennessee
in
Partial Fulfillment of the Requirements
for the degree of
Master of Arts

---

by

Helen Bradley Grimble

March 1950

ACKNOWLEDGMENT

The author wishes to express her appreciation for the valuable assistance rendered her by Professor D. D. Miller, under whose direction this paper was written.

0. Introduction.

The concept of prime ideal, which arises in the theory of rings as a generalization of the concept of prime number in the ring of integers, plays a highly important role in that theory, as might be expected from the central position occupied by the primes in arithmetic. In the present paper, the concept is defined for ideals in semigroups, the simplest of the algebraic systems of single composition, and some analogies and differences between the ring and semigroup theories are brought out. We make only occasional references to ring theory, however; a reader acquainted with that theory will perceive its relation to our theorems without difficulty, and a reader unacquainted with it will find that the logical development of our results is entirely independent of it.

Our first section is a collection of definitions of basic terms and well known theorems concerning semigroups. The second is devoted to a few theorems on divisors of identity elements, and the third to zero divisors. In the fourth, we introduce prime ideals, and discuss their unions, intersections, and products. The fifth section concerns prime ideals in semigroups with identity elements, and in the sixth we consider relations between prime ideals and maximal ideals.

Throughout the paper we have occasion to consider "one-sided" concepts. It will be clear that any theorem involving such notions may be converted into another of the same truth-value by interchanging throughout the words "left" and "right."

1. Preliminaries.

We shall avail ourselves of the standard terminology and notation of the theory of sets, with which we assume the reader to be acquainted. In particular, we shall use capital Roman letters to denote sets, small Roman letters for their elements, small Greek letters for mappings, $\in$ for the relation of elementhood, $\subseteq$ for inclusion, $\subset$ for proper inclusion, $\cup$ for union (= class sum = set-theoretic sum), $\cap$ for intersection, and $\emptyset$ for the null set; when all sets under discussion are subsets of some set S, we shall denote by $C(A)$ the complement of A with respect to S. The symbol $=$ will be used both for a relation between sets and for a relation between elements: $A = B$ will mean that both $A \subseteq B$ and $B \subseteq A$, and $a = b$ will mean that a and b are the same element; it may be noted that equality (logical identity) of elements may often be replaced by an equivalence relation, or at least by a regular[1] equivalence, but we shall not advert to this fact in the sequel. We also assume that the reader is familiar with such ordinary algebraic notions as that of arithmetical congruence, denoted by $\equiv$.

---

[1]For definition and properties of regular equivalence relations, see Paul Dubreil, Algebre, v. I (Paris: Gauthier-Villars, 1946), p. 80. For an axiomatic treatment of semi-groups in which an equivalence relation replaces equality, see H. S. Vandiver, "The Elements of a theory of abstract discrete Semi-groups," Vierteljahrsschrift der Naturforschenden Gesellschaft in Zurich, 85 (1940), pp. 71-86.

Definition 1.1. A semigroup is a system consisting of a non-empty set S and a single-valued binary associative operation which associates with each ordered pair of elements of S an unique element of S. Ordinarily, we shall call this operation multiplication, and call the element associated with an ordered pair of elements a, b their product, written $a \cdot b$ or ab. In this notation, the associativity of the operation is described by the equality $a(bc) = (ab)c$ for all elements a, b, c of S. If $ab = ba$ we say that the elements a and b commute with each other; if $ab = ba$ for all elements[2] $a, b \in S$, we call[3] S a commutative semigroup. Occasionally we may find it convenient to write $a + b$ instead of ab, in which case we speak of an additive instead of a multiplicative semigroup, but we shall do so only when referring to commutative semigroups. The order of a semigroup is the cardinal number of its set of elements.

A few well-known examples of semigroups may be mentioned: (1) all integers, under addition or under multiplication; (2) the positive integers greater than some fixed integer k, under addition or under multiplication; (3) all real functions on a given interval (finite or infinite) under multiplication, the product fg of two such functions being

---

[2]It will be convenient to use the notation "$a,b \in S$" as an abbreviation for "$a \in S$ and $b \in S$".

[3]No confusion need arise from the use of S to denote the semigroup as well as the set of all its elements.

defined to be the function whose value at any point a of the given interval is $f(a) \cdot g(a)$; (4) the integers under multiplication modulo n ; (5) all $m \times n$ matrices (for fixed m and n) over an arbitrary ring, under matrix addition; (6) all square matrices of order n over an arbitrary ring, under matrix multiplication; (7) all single-valued mappings of a set E into itself, under iteration (*i.e.*, consecutive performance of mappings). The first five of these are examples of commutative semigroups; the first three are examples of infinite semigroups, and the fourth of a finite semigroup; (5) and (6) are finite if the ring is finite, otherwise infinite; and (7) is finite if the set E is finite, otherwise infinite. Additional examples will be found in the Appendix, which is a list, compiled by K. S. Carman, J. C. Harden, and E. E. Posey, of all semigroups of orders less than five; we shall refer to these semigroups by number, semigroup m.n being the n^{th} in the list of semigroups of order m .

If a subset S_1 of a semigroup S is itself a semigroup under the defining operation in S , S_1 will be called a *subsemigroup* of S . Since associativity holds throughout S , it holds in S_1 , and a necessary and sufficient condition that a subset S_1 of S be a subsemigroup of S is that S_1 be closed under the multiplication defined in S . If S_1 is a subsemigroup of S and $S_1 \subset S$, we shall say that S_1 is a proper subsemigroup of S . Clearly, if S_2 is a subsemigroup of S_1 and S_1 is a subsemigroup of S then S_2 is a subsemigroup of S . Thus, in Example (2) above, the even integers in the semigroup form a subsemigroup regardless of whether addition or multiplication is chosen as the defining operation, while the odd integers form a subsemigroup under multiplication but not under addition; and the entire semigroup (2), in turn, under either operation is a subsemigroup of (1) under the same operation. The other examples listed above also contain noteworthy subsemigroups: the continuous functions on the interval are a subsemigroup of (3); the integral multiples of d, where d is a divisor of n, are a subsemigroup of (4); the matrix all of whose elements are zero constitutes by itself a subsemigroup of (5); the nonsingular matrices in (6) form a subsemigroup, and the singular matrices form another; in (7) the one-to-one mappings constitute a subsemigroup.

It is obvious that the intersection of an arbitrary collection of subsemigroups of a semigroup S is empty or a subsemigroup of S. But the union of subsemigroups need not be a subsemigroup; for example, in the additive semigroup of integers modulo 6, if S_1 consists of the multiples of 2, and S_2 of the multiples of 3, then $2 + 3 = 5 \notin S_1 \cup S_2$.

<u>Definition 1.2</u>. In a semigroup S, an element e such that $ex = x$ for every $x \in S$ is called a <u>left identity element of</u> S. Dually, an element f such that $xf = x$ for every $x \in S$ is called a <u>right identity element of</u> S. If e

is both a left identity element and a right identity element of S, *i.e.*, if $xe = ex = x$ for all $x \in S$, then e is called a *two-sided identity element of* S, or simply an *identity element of* S. A semigroup S may have any number of left (or of right) identity elements; but if it has at least one left identity element e and at least one right identity element f then $e = ef = f$, whence S has an unique two-sided identity element and no other left or right identity element.

Definition 1.3. In a semigroup S, an element y such that $yx = y$ for every $x \in S$ is called a *left zero element*[4] *of* S, and an element z such that $xz = z$ for every $x \in S$ is called a *right zero element of* S. If $xz = zx = z$ for every $x \in S$, so that z is both a left and a right zero element of S, then z is called a *two-sided zero element*, or simply a *zero element*, of S. A semigroup S may have any number of left (or of right) zero elements, but if it has a left zero element y and a right zero element z then $y = yz = z$, whence S has an unique two-sided zero element and no other left or right zero element.

Definition 1.4. An element a of a semigroup S is said to be *idempotent* if $a^2 = a$. If $a, b \in S$ and $a^n = b$,

---

[4] Some writers prefer the term *annihilator* or *annulator* instead of "zero element," presumably to avoid confusion with the identity element of an additive semigroup. Cf. Vandiver, *op. cit.*, p. 76.

where n is a positive integer,[5] then a is called an n^{th} root of b ; the roots of a two-sided zero element of S are called nilpotent elements. An idempotent element a is obviously an n^{th} root of a for every positive integer n . The square roots of a left or right identity element of S are often called involutory elements. Clearly, all left and right identity elements, and all left and right zero elements, are idempotent, and the former are involutory.

Definition 1.5. If a and b are elements of a semigroup S , and if there exists an element $x \in S$ such that $ax = b$, then a is said to be a left divisor of b ; if $ya = b$ for some $y \in S$, then a is said to be a right divisor of b ; if a is both a left and a right divisor of b , it is called a two-sided divisor of b . If a is a left divisor of every element of S , we may call it a universal left divisor of S ; universal right divisors and universal two-sided divisors of S are defined similarly. If $a \neq b \neq x$ and $ax = b$, we say that a is a proper left divisor of b ; proper right divisors and proper two-sided divisors are defined similarly. Every left (right) identity element of S is of course a universal left (right) divisor of S , and any n^{th} root $(n > 1)$ of an element b is a two-sided divisor of b (in

---

[5]Positive integral powers of an element of a semigroup are defined in the usual way ($b^1 = b$; $b^n = bb^{n-1}$ for $n > 1$) and obey the rules $b^m b^n = b^{m+n} = b^n b^m$ and $(b^m)^n = b^{mn}$, each of which can be derived from closure and associativity by an easy inductive argument. Non-integral exponents and integral non-positive exponents are not defined for elements of general semigroups.

particular, any idempotent element is a two-sided divisor of itself). If S contains a right (left) identity element e then every element $a \in S$ is a left (right) divisor of itself, for $ae = a$ $(ea = a)$. But in the absence of the appropriate identity elements, an element need not divide itself. For example, in No. 4.68 there are two right identity elements (1 and 2), which of course are universal right divisors of the semigroup, and each is a two-sided divisor of itself since each is idempotent; but neither is a left divisor of the other. The element 3 in this semigroup is idempotent (in fact, it is a two-sided zero element) and hence is a two-sided divisor of itself. But the semigroup has no left identity element, and the element 4 , although a left divisor of itself, is not a right divisor of itself. It may be remarked that an element (such as 4 in No. 4.44) may be a two-sided divisor of itself without being idempotent.

Definition 1.6. The usual definition of group may be formulated in our present terminology as follows: a group G is a semigroup containing a left identity element e of which every element of G is a right divisor. Under these conditions it follows readily[6] that e is a (necessarily unique)

---

[6]For a neat proof, see Hans Zassenhaus, Lehrbuch der Gruppentheorie, v. I (Leipzig u. Berlin: Teubner, 1937), p. 2. [English translation, The Theory of Groups (New York: Chelsea, 1949), same page.]

two-sided identity element of G and that for each $a \in G$ there is an unique <u>inverse element</u> a^{-1} such that $a^{-1}a = aa^{-1} = e$. An equivalent definition[7] states that a group G is a semigroup in which, for arbitrary $a, b \in G$, the equations $ax = b$ and $ya = b$ are solvable; the uniqueness of the solutions is easily proved. In our present terminology the latter definition may be stated thus: a group is a semigroup in which each element is a two-sided divisor of every element. We note that a group cannot contain either a left or a right zero element, and that its only idempotent element is the identity. Commutative groups are usually referred to as <u>abelian</u>. If a group G is a subsemigroup of a semigroup S, we shall say that G is a <u>subgroup</u> of S. In any group the cancellation laws hold: $ax = ay$ implies $x = y$, and $xa = ya$ implies $x = y$; conversely, a finite semigroup in which both cancellation laws hold is a group,[8] but this need not be true for infinite semigroups (<u>e.g.</u>, the multiplicative semigroup of all positive integers).

<u>Definition 1.7</u>. The <u>product</u> AB of non-empty subsets A and B of a semigroup S is defined to be the set of all elements ab, where $a \in A$ and $b \in B$. It is almost an

---

[7]The equivalence of these definitions was first noted by E. V. Huntington, "Simplified definition of a group," Bull. Amer. Math. Soc. 8 (1901-2), pp. 296-300. A proof is given in Zassenhaus, <u>op. cit.</u>, p. 3.

[8]For a proof, see Zassenhaus, <u>loc. cit.</u>

immediate consequence[9] of the associativity of the multiplication of elements defined in S that the multiplication of subsets is associative: $A(BC) = (AB)C$. The following rules of calculation, which we shall use constantly, we shall list without proof:[10] (1) if $A_1 \subseteq A$ and $B_1 \subseteq B$, then $A_1B_1 \subseteq AB$; (2) if $\mathfrak{M}$ is any class of subsets then $A \cdot \bigcup_{M \in \mathfrak{M}} M = \bigcup_{M \in \mathfrak{M}} AM$; (3) $A \cdot \bigcap_{M \in \mathfrak{M}} M \subseteq \bigcap_{M \in \mathfrak{M}} AM$. The inclusion relation in (3) is not in general reversible.[11]

Definition 1.8. In terms of multiplication of subsets, subsemigroups of a semigroup S may be characterized as non-empty subsets A such that $A^2 \subseteq A$. If the stronger condition $AS \subseteq A$ is satisfied, A is called a right ideal of S ; if $SA \subseteq A$ then A is called a left ideal of S ; if A is both a right and a left ideal of S it is called a two-sided ideal of S . If A is a two-sided ideal of S then $SAS = (SA)S \subseteq AS \subseteq A$. Conversely, if $SAS \subseteq A$ and S has a left identity element e then $AS = eAS \subseteq SAS \subseteq A$, so that A is a right ideal of S ; dually, if S has a right

---

[9]A detailed proof is given in W. A. Rutledge's University of Tennessee Master's Thesis, Normality in Semigroups, 1948, p. 4.

[10]For proofs, see Dubreil, op. cit., p. 31.

[11]A finite example in which the left-hand side of the inclusion is empty while the right-hand side is not may be found in No. 4.49; it is discussed in detail in K. S. Carman's University of Tennessee Master's Thesis, Semigroup Ideals, 1949, p. 11. An example in which both sides are non-empty is given by Dubreil, op. cit., p. 32.

identity element and $SAS \subseteq A$ then A is a left ideal of S ; hence if S has a two-sided identity element and $SAS \subseteq A$ then A is a two-sided ideal of S . But, in the absence of appropriate identity elements, $SAS \subseteq A$ need not imply either $SA \subseteq A$ or $AS \subseteq A$. For example, in the commutative semigroup whose multiplication table[12] is exhibited below, let A be the subset [1 2 3 4] . Then $SAS = S^2A = [1\ 2\ 4\ 5]\cdot[1\ 2\ 3\ 4] = [1\ 4] \subset A$; but $AS = SA = [1\ 2\ 4\ 5] \not\subset A$.

	1	2	3	4	5	6
1	1	1	1	4	4	4
2	1	1	1	4	4	4
3	1	1	2	4	4	5
4	4	4	4	1	1	1
5	4	4	4	1	1	1
6	4	4	5	1	1	2

However, it should be noticed that, for an arbitrary non-empty subset A of S , the subsets SA , AS , and SAS are respectively left, right, and two-sided ideals of S .

Any left (right) zero element of S is evidently contained in every left (right) ideal of S , and hence in every

---

[12]This semigroup was found in J. C. Harden's University of Tennessee Master's Thesis, Direct and Semidirect Products of Semigroups, 1949, p. 14. It is the direct product (a term we shall define later) of Nos. 2.1 and 3.2.

two-sided ideal; any two-sided zero element therefore lies in every ideal. Indeed, a left (right, two-sided) zero element is itself a right (left, two-sided) ideal; and any left (right, two-sided) ideal consisting of a single element is a right (left, two-sided) zero element.

We cite without proof[13] the following well-known and fundamental theorems concerning ideals, of which we shall make constant use: (1) the product of two left (right, two-sided) ideals of S is a left (right, two-sided) ideal of S [this statement can obviously be extended to the product of any finite set of left (right, two-sided) ideals, taken in any order]; (2) if L is a left ideal and R a right ideal of S, then LR is a two-sided ideal of S, but RL need be neither a left nor a right ideal of S (cf. No. 4.64); (3) the intersection of any collection of left (right, two-sided) ideals of S is either the null set or a left (right, two-sided) ideal of S, but the intersection of a left ideal and a right ideal need not be an ideal (cf. No. 4.111); (4) the intersection of any finite collection of two-sided ideals of S is a two-sided ideal of S, and furthermore the intersection contains all the products obtained by multiplying all the ideals in the collection in any order; (5) the union

[13] These results are easily obtained. Perhaps the least obvious is the fact that (even in the absence of a zero element) the intersection of a finite collection of two-sided ideals is non-empty; a detailed proof may be found in Carman, op. cit., p. 13.

of any collection of left (right, two-sided) ideals of S is a left (right, two-sided) ideal of S . That (4) fails if the finiteness condition be dropped is shown by the following example: let S be the additive semigroup of all positive integers, and let A_k be the set of integers greater than k (k = 1, 2, . . .); then each A_k is a two-sided ideal of S , but $\bigcap_{k \in S} A_k = \emptyset$. Furthermore, (4) need not hold for one-sided ideals, for left (right) ideals may be disjoint (<u>cf</u>. no. 4.66); however, it follows from (2) that if S contains at least one left ideal L and at least one right ideal R then S contains at least one two-sided ideal, and since $RL \subseteq L \cap R$ it follows that every left ideal intersects every right ideal.

The <u>principal left ideal generated by an element</u> $b \in S$ is the ideal Sb ; if S contains a left identity element e , then $b = eb \in Sb$, but in the absence of a left identity element we may have $b \notin Sb$ (for example, the principal ideal generated by 2 in the multiplicative semigroup of even integers). Dually, the <u>principal right ideal generated by</u> b is defined to be bS ; and if S contains a right identity element then $b \in bS$. We also define the <u>principal two-sided ideal generated by</u> b to be SbS , which contains b if S contains a two-sided identity element.

<u>Definition 1.9</u>. A subset A of a set M is said to be <u>maximal in M with respect to a property</u> P if A is

not a proper subset of any proper subset of M having property P. Thus, A is a maximal subsemigroup (subgroup, ideal) of a semigroup S if $A \subset B \subseteq S$, where B is a subsemigroup (subgroup, ideal) of S, implies $B = S$.

Definition 1.10. If a is an element of a semigroup S, and if, for all $x, y \in S$, $ax = ay$ implies $x = y$, then a is said to be left cancellable in S; dually, if $xa = ya$ necessarily implies $x = y$, a is right cancellable in S. A cancellable element is one which is both left and right cancellable. We have already remarked (Definition 1.6) that if every element of a finite semigroup S is cancellable then S is a group.

2. Divisors of identity.

We proceed now to a few theorems on left and right divisors of left and right identity elements. In most cases we shall state only one of each pair of dual theorems.

Theorem 2.1. *If e is either a left identity element or a right identity element of a semigroup S, and if b is a root of e, then the left divisors of b form a subsemigroup of S.*

Proof. Let $cx = dy = b$. By hypothesis, $b^n = e$ for some positive integer $n \geq 2$; for if $b = e$ then $b^2 = e^2 = e$. Now

$(cd)(yb^{n-1}x) = c(dy)b^{n-1}x = cbb^{n-1}x = cb^nx = cex$. But if e is a left identity element then $cex = c(ex) = cx = b$; and if e is a right identity element then $cex = (ce)x = cx = b$. Hence, in either case, $(cd)(yb^{n-1}x) = b$, whence cd is a left divisor of b.

By left-right duality, the right divisors of a left or right identity element b form a semigroup; and since the set of two-sided divisors of b is just the intersection of the semigroups of left and of right divisors, the two-sided divisors also constitute a semigroup.

In particular (and this is the case in which we are most interested) the left (right, two-sided) divisors of a left or right identity element constitute a subsemigroup of S.

We remark that while in a commutative semigroup the idempotent elements (and, more generally, the elements a such that $a^n = a$, where n is a fixed positive integer) constitute a subsemigroup, this need not be the case in a non-commutative semigroup. For example, in No. 4.113 the elements 1, 2, and 4 are idempotent, while 3 is not, but $4 \cdot 2 = 3$.

Theorem 2.2. _If a semigroup_ S _contains at least one left identity element, then all left identity elements of_ S _have a common set_ D _of left divisors, and_ D _is exactly the set of all universal left divisors of_ S. _Furthermore,_ D _is a semigroup and contains as a subsemigroup the set_ E *of all left identity elements of* S *; the set of left identity elements of* D *is just* E *, which is also the set of all idempotent elements in* D .

Proof. Let e be a left identity element of S , let $dx = e$, and let $s \in S$. Then $d(xs) = (dx)s = es = s$, whence d is a left divisor of the arbitrary element s , and hence is a universal left divisor of S . It is trivial that, conversely, any universal left divisor of S is a left divisor of the arbitrary left identity element e . By Theorem 2.1, D is a semigroup; and since any left identity element is a left divisor of itself, $E \subseteq D$. But if e and f are left identity elements of S then $ef = f \in E$, whence E is a subsemigroup of D . Let c be a left identity element of D , let $d \in D$, let $e \in E$, and let $s \in S$; then $dx = e$ for some $x \in S$. Now

$cs = c(es) = ces = c(dx)s = (cd)(xs) = d(xs) = (dx)s = es = s$,

whence c is a left identity element of S , *i.e.*, $c \in E$; the converse is trivial. Hence E is the set of all left identity elements of D . Finally, if $d \in D$ and $s \in S$ then $dx = s$ for some $x \in S$; hence if $d^2 = d$ we have $s = dx = d^2x = d(dx) = ds$, whence $d \in E$. Conversely, every element of E is idempotent, so we conclude that E is the set of all idempotent elements of D .

Corollary. A commutative semigroup S *has an identity element if and only if* S *contains at least one universal* *divisor. If S has an identity element e, the divisors of e are just the universal divisors of S, and they form a subsemigroup of S.*

Proof. An identity element of S is itself a universal divisor of S. Conversely, if d is a universal divisor of S, then d divides itself, so that $dc = d$ for some $c \in S$; and if $s \in S$ then $xd = s$ for some $x \in S$. Now $sc = (xd)c = x(dc) = xd = s$, whence c is an identity element of the commutative semigroup S. The rest of the Corollary follows immediately from Theorem 2.2.

Theorem 2.3. The left cancellable elements of a semigroup S form a semigroup, of which the right divisors of any left identity element of S constitute a subsemigroup.

Proof. Let a and b be left cancellable elements of S. Then, for any $x, y \in S$, $ax = ay$ and $bx = by$ each imply $x = y$. Hence $(ab)x = (ab)y$ implies $a(bx) = a(by)$, which by hypothesis implies $bx = by$, and this implies $x = y$. Hence the left cancellable elements of S form a semigroup C. If e is a left identity element of S, the right divisors of e are left cancellable in S; for if $sd = e$ and $x, y \in S$ then if $dx = dy$ we have
$x = ex = (sd)x = s(dx) = s(dy) = (sd)y = ey = y$, whence d is left cancellable. But, by Theorem 2.1, the right divisors of e form a semigroup, and hence a subsemigroup of C.

No. 4.65 assures us that the right divisors of a left identity element may be a proper subsemigroup of the left cancellable elements, for here the only left identity element is 3 , and its only right divisors are 3 and 4 , but every element of the semigroup is left cancellable.

We remark that if a semigroup S contains a left identity element and a right cancellable element then the left identity element is unique. For, if e and f are left identity elements and a is right cancellable in S , then $ea = a = fa$, whence $e = f$.

Corollary. *In a finite commutative semigroup S , the cancellable elements form a group C ; and if S has an identity element e then the divisors of e form a subgroup of C .*

Proof. Since C is a finite semigroup (by Theorem 2.3) in which the cancellation laws hold, C is a group. But, as is well known,[14] any subsemigroup of a finite group is a subgroup. Hence, by Theorem 2.3, the divisors of e constitute a subgroup of C .

We shall improve upon the second half of this Corollary shortly, by showing that even in a non-commutative finite semigroup the right divisors of any left identity element

---

[14]See, for example, Garrett Birkhoff and Saunders MacLane, *A Survey of Modern Algebra* (New York: Macmillan, 1941), p. 143.

form a group. But before proceeding to this and other theorems on divisors of identity in finite semigroups we present a theorem of Rees,[15] which we shall find useful and which may be of some interest on its own account. We have added slight embellishments to the theorem, and we give a new and quite detailed proof. We first adopt

Definition 2.1. A semigroup all of whose elements are positive integral powers of some element b is called a cyclic semigroup. If all the elements in the infinite sequence b, b^2, b^3, . . . are distinct, then the correspondence $b^i \leftrightarrow i$ between the elements of the semigroup $b, b^2, b^3, \ldots$ and the additive semigroup of positive integers is an isomorphism, for $b^i b^j = b^{i+j} \longleftrightarrow i + j$.

Theorem 2.4. Every finite cyclic semigroup contains an unique maximal subgroup, which is cyclic and is the intersection of all ideals of the semigroup.

Proof. Let B be the cyclic semigroup $b, b^2, b^3, \ldots$ generated by b . By the associative law, B is commutative. If $i \neq j$ implies $b^i \neq b^j$ for all positive integers i and j , then B is the (unique) infinite cyclic semigroup, and is isomorphic to the additive semigroup of positive integers. Hence if B is finite there exist positive integers i and j such that $i \neq j$ and $b^i = b^j$. Let n be the

[15] D. Rees, "On Semi-groups," Proc. Camb. Phil. Soc., 36(1940), p. 388.

least positive integer such that $b^n = b^k$ for some $k < n$; then if $k \neq i < n$ we have $b^n \neq b^i$, for if $b^n = b^i$ then $b^i = b^k$ with both $i < n$ and $k < n$, contrary to the choice of n . Hence the elements $b, b^2, \ldots, b^{n-1}$ are distinct. Let $m = n - k$; we show now that if j and q are positive integers and $j \geq k$ then $b^j b^{qm} = b^j$, and later that if $j < k$ then $b^j b^t \neq b^j$ for every positive integer t . Assuming $j \geq k$, we may write $j = k + s$, where s is a non-negative integer. If $s = 0$ and $q = 1$, $b^j b^{qm} = b^k b^m = b^{k+m} = b^n = b^k = b^j$. If $s = 0$ and $q > 1$, we make the inductive assumption that $b^k b^{(q-1)m} = b^k$. But $b^k b^{qm} = b^k b^{(q-1)m} b^m = b^k b^m = b^k$, whence the induction is complete and $b^k b^{qm} = b^k$ for every positive integer q . Now if t is any positive integer and $b^k b^t = b^k$ then if $s > 0$ we have $b^{k+s} b^t = b^k b^t b^s = b^k b^s = b^{k+s}$. Letting $t = qm$, we see that for any positive q and non-negative s , $b^{k+s} b^{qm} = b^{k+s}$. Hence

$$(1) \qquad b^j b^{qm} = b^j , \qquad j \geq k , \quad q > 0 .$$

Let p be a non-negative integer, and let $p = qm + r$, where q and r are non-negative integers and $r < m$. We show now that $b^{k+p} = b^{k+r}$. If $p < m$ then $r = p$, and the result is trivial. If $p \geq m$ and $p \equiv 0 \pmod{m}$ then $p = qm$, $q > 0$, and by (1) we have $b^{k+p} = b^{k+qm} = b^k b^{qm} = b^k = b^{k+0} = b^{k+r}$. If $p > m$ and $p \not\equiv 0 \pmod{m}$ then $q > 0$, $r > 0$, and $b^{k+p} = b^{k+qm+r} = b^k b^{qm} b^r = b^k b^r = b^{k+r}$. Since $r < m$,

$k + r < k + m$, and an immediate consequence is that the $n - 1$ elements $b, b^2, \ldots, b^{k+m-1}$ constitute the whole of B . Furthermore, if $j < k$ then $b^j \neq b^i$ for all positive integers i, $i \neq j$. It follows immediately, as forecast in the preceding paragraph, that if $j < k$ then $b^j b^t \neq b^j$ for all positive integers t .

Now we show that <u>if</u> u <u>and</u> v <u>are non-negative integers then</u> $b^{k+u} = b^{k+v}$ <u>if and only if</u> $u \equiv v \pmod{m}$. Let $u = q_1 m + r_1$ $(q_1 \geq 0 , \; 0 \leq r_1 < m)$ and $v = q_2 m + r_2$ $(q_2 \geq 0 , \; 0 \leq r_2 < m)$. Then $b^{k+u} = b^{k+r_1}$ and $b^{k+v} = b^{k+r_2}$, whence if $b^{k+u} = b^{k+v}$ then $b^{k+r_1} = b^{k+r_2}$. But $0 < k + r_i \leq k + m$ $(i = 1, 2)$, whence $k + r_1 = k + r_2$, $r_1 = r_2$. Hence $u - v = (q_1 - q_2)m$, so that $u \equiv v \pmod{m}$. Conversely, if $u \equiv v \pmod{m}$ then $r_1 = r_2$, whence $b^{k+u} = b^{k+r_1} = b^{k+r_2} = b^{k+v}$.

We now prove a converse of (1): if j and t are positive integers and $b^j b^t = b^j$ then $t = qm$ for some positive integer q . If $b^j b^t = b^j$ then, as we have seen, $j \geq k$; hence $b^{k+(j-k+t)} = b^{j+t} = b^j b^t = b^j = b^{k+(j-k)}$, whence by the preceding paragraph $j - k + t \equiv j - k \pmod{m}$, whence $t \equiv 0 \pmod{m}$. But $t > 0$, so that $t = qm$ for some positive integer q . Combined with (1), this result yields the following: <u>if</u> j <u>and</u> t <u>are positive integers then</u> $b^j b^t = b^j$ <u>if and only if both</u> $j \geq k$ <u>and</u> $t = qm$ <u>for some positive integer</u> q.

Let G denote the set $b^k, b^{k+1}, \ldots, b^{k+m-1}$ of m distinct elements. We have already seen that if $i \geq k$ then $b^i \in G$, whence G is closed under multiplication and so is a subsemigroup of B. We proceed to prove that G is a group; since B (and hence G) is commutative, we need only prove that for arbitrary $b^i, b^j \in G$ the equation $b^i x = b^j$ is solvable in G. Let $k = q'm + r$, $q' \geq 0$, $0 \leq r < m$, and let $q = 2 + q'$. Then $qm = (2 + q')m = 2m + q'm = 2m + k - r$, and, since $r < m$, $qm > 0$. Since $b^i, b^j \in G$, we may take $k \leq i \leq k + m - 1$ and $k \leq j \leq k + m - 1$, whence $j - i \geq 1 - m$. Hence, since $- r \geq 1 - m$,

$$qm + j - i = 2m + k - r + j - i \geq 2m + k + (1 - m) + (1 - m) = k + 2,$$

whence $b^{qm+j-i} \in G$. But $b^i b^{qm+j-i} = b^{qm+j} = b^{qm} b^j = b^j$, so that $x = b^{qm+j-i}$ is the desired solution, and therefore G is a group and the solution is unique in G. The exponent $qm+j-i$ is not unique, of course, for $b^{pm+j-i} = b^{qm+j-i}$ for any integer $p \geq q$. It may be that $qm + j - i > k + m - 1$, and it might seem desirable to give the solution in the form b^t with $k \leq t \leq k + m - 1$; but this is not possible in general (i.e., for all i and j in the range from k to $k + m - 1$), as the following argument shows. If $b^t = b^{qm+j-i}$ then $t \equiv qm + j - i \equiv j - i \pmod{m}$, whence $t = pm + j - i$ for some integer p. If $p < q$ then

$pm \leq (q - 1)m = (1 + q')m = m + q'm = m + k - r$, and $pm + j - i \leq m + k - r + j - i$. But if $r \geq 2$ and

$j - i = 1 - m$ then $m + k - r + j - i \leq k - 1$, and $t = pm + j - i \leq k - 1$, whence $b^t \notin G$. Hence b^t, where $t < qm + j - i$, is not a solution in G for all choices of i and j unless $r < 2$. But if $r < 2$ and $p = q - 1 = 1 + q'$ then $pm = m + k - r > k + m - 1$; and if $j - i > o$ then $t = pm + j - i > k + m - 1$, whence t lies outside the range from k to $k + m - 1$. The remaining possibility is the case $r < 2$, $p < q - 1$. But if $p \leq q - 2 = q'$, then $r < 2$ implies $pm \leq q'm = k - r \leq k$, whence $t = pm + j - i \leq k + j - i$, so that if $j - i < o$ then $t < k$; hence either $t \leq o$ and b^t is not defined, or $o < t < k$ and $b^t \notin G$. We conclude that for no cyclic semigroup B is it possible to write the solution of $b^i x = b^j$, for all i and j, in the form b^t where $k \leq t \leq k + m - 1$.

Defining q, as in the preceding paragraph, to be $2 + (k - r)/m$, where r is the least non-negative residue of k modulo m, it is obvious that the identity element of G is b^{qm}, where $qm = 2m + k - r$. Even when $2m + k - r$ is as small as possible (i.e., when $r = m - 1$ and $2m + k - r = k + m + 1$), $qm > k + m - 1$; hence qm is never in the range from k to $k + m - 1$. However, $(q - 1)m = (1 + q')m > o$ and $b^i b^{(q-1)m} = b^i$ for all $i > k$, so that $b^{(q-1)m}$ is the identity element of G. And since $o \leq r \leq m - 1$ and $(q - 1)m = k + m - r$, we have $k + 1 \leq (q - 1)m \leq k + m$. Hence $b^{(q - 1)m}$ represents the identity element of G in a form in which the exponent lies in the range from k to $k + m - 1$ unless the identity element is b^k, in which case it is represented as b^{k+m}. Clearly, no smaller exponent than $(q - 1)m$ will suffice, for if $b^t = b^{(q-1)m}$ then $t \equiv (q - 1)m \equiv o \pmod{m}$, so that the greatest eligible t less than $(q - 1)m$ is $(q - 2)m$; but $(q - 2)m = q'm$, and if $q' = o$ then $b^{(q-2)m}$ is not defined.

The inverse of an element $b^i \in G$ is given by $b^{(2q-1)m-i}$; for

$$b^i b^{(2q-1)m-i} = b^{(2q-1)m} = b^{(q-1)m+qm} = b^{(q-1)m}\, b^{qm} = b^{(q-1)m};$$

and since $i < k + m$ and $r < m$ we have

$$(2q - 1)m - i > (2q - 1)m - k - m = 2qm - 2m - k = 2m + k - 2r > k,$$

so that $b^{(2q-1)m-i} \in G$. No smaller exponent than $(2q - 1)m - i$ will suffice for the inverses of all b^i; for, as we have argued before, if $b^i b^t = b^{(q-1)m}$ then $t \equiv (q - 1)m - i \pmod{m}$, and the greatest such $t < (2q - 1)m - i$ is $(2q - 2)m - i$; but if $i = k + m - 1$ and $r = m - 1$ then

$$(2q-2)m-i = (2q-2)m-k-m+1 = 2qm-3m-k+1 = m+k-2r+1 = k-m+3,$$

whence if $m > 3$ then $(2q -2)m - i < k$ and $b^{(2q-2)m-i} \notin G$.

We observe that, since $b^j b^i \in G$ for all $j > o$ and all $b^i \in G$, G is not only a group but an ideal (necessarily two-sided since B is commutative) of B, and hence[16] is the zeroid group (i.e., the intersection of all two-sided ideals) of B. It follows that, for every $b^j \in B$ and every $b^i \in G$, the equation $b^j x = b^i$ has a solution in G. It also follows[17] that any group contained in B but not contained in G must lie entirely outside G, and from this we conclude that every group in B is a subgroup of G; for if G' is a group lying outside of G, and b^h is the element of G' having the greatest exponent, then $(b^h)^2 = b^{2h} \notin G'$ since by hypothesis $G \neq B$ and so $h \neq 1$. Thus G is the unique maximal subgroup of B.

Finally, we prove that the group G is cyclic. Among the integers of the form $xm + 1$, select the least one not less than k, and call it $tm + 1$. Since $tm + 1 \geq k$, $b^{tm+1} \in G$. Now $(b^{tm+1})^m = b^{m(tm+1)}$ is the identity element of G since $tm + 1 \geq k$. On the other hand, if $(b^{tm+1})^s = b^{s(tm+1)}$ is the identity element, for some positive integer s, then $s(tm + 1) \equiv 0 \pmod{m}$; and, since $tm + 1$ is prime to m, this implies $s \equiv 0 \pmod{m}$, i.e., $s = hm$ for some positive integer h. Hence the least positive integer s such that $(b^{tm+1})^s$

---

[16]For definition and properties of the zeroid group, see A. H. Clifford and D. D. Miller, "Semigroups having zeroid elements," Amer. Jour. Math., 70(1948), pp. 117-25.

[17]*Ibid.*, p. 123.

is the identity element of G is m. Thus the order of the element b^{tm+1} equals the order of the group, whence b^{tm+1} generates G, and G is cyclic.

Corollary 1. Every finite semigroup contains at least one idempotent element.

Corollary 2. Every subgroup of a cyclic semigroup is cyclic.

Proof. The infinite cyclic semigroup has no idempotent element and hence no subgroup, whence the corollary is true vacuously. In a finite cyclic semigroup, we have shown that every group is a subgroup of a cyclic group, and it is well known[18] that every subgroup of a cyclic group is cyclic.

Definition 2.2. We shall say that an element b of a semigroup is *of finite order* if the cyclic semigroup generated by b is finite, and that the order of this cyclic semigroup is the *order* of b.

Lemma 2.1. *If a universal left divisor b of a semigroup S is of finite order, then the cyclic semigroup B generated by b is a group.*

Proof. By Theorem 2.4, B contains an unique maximal subgroup G consisting of the powers b^k, b^{k+1}, . . . , b^{n-1}, where n is the least positive integer

[18] See, for example, Zassenhaus, *op. cit.*, p. 15.

such that $b^n = b^k$ for some $k < n$. Now if $k = 1$ then $G = B$ and our result is attained. If $k > 1$, we show first that b^k is a left divisor of b. Since b is a universal left divisor of S, we may write $b = bd$ for some $d \in S$, and $d = bc$ for some $c \in S$. Now $b = bd = b(bc) = b^2c$, whence b^2 is a left divisor of b. We make the inductive assumption that b^{k-1} is a left divisor of b; then, for some $a \in S$, we have $b = b^{k-1}a$. But $a = br$ for some $r \in S$, whence $b = b^{k-1}a = b^{k-1}br = b^kr$. Thus by complete induction we have shown that b^k is a left divisor of b. Now let b^q $(k \leq q < n)$ be the identity element of G. Then $b^qb = b^q(b^kr) = (b^qb^k)r = b^kr = b$. But we have seen in proving Theorem 2.4 that $b^qb^i = b^i$ if and only if $i \geq k$, *i.e.*, if and only if $b^i \in G$. Hence $b \in G$ and $G = B$.

Theorem 2.5. A semigroup S *has a left identity element if and only if* S *contains a universal left divisor of finite order.*

Proof. The necessity is immediate, for any left identity element is a universal left divisor of S and generates a group of order 1. To prove the sufficiency, let b be a universal left divisor of finite order. Now, by Lemma 2.1, b generates a group G; let e be the identity element of G, and let $s \in S$. Then $bx = s$ for some $x \in S$, and $es = e(bx) = (eb)x = bx = s$, whence e is a left identity element of S.

Corollary. *A finite semigroup S has a left identity element if and only if S has a universal left divisor.*

Lemma 2.2. *In a finite semigroup S, an element b is left cancellable in S if and only if b is a universal left divisor of S.*

Proof of necessity. Let the distinct elements $s_1, \ldots, s_n$ be all the elements of S. By hypothesis, $i \neq j$ implies $bs_i \neq bs_j$ $(i, j = 1, \ldots, n)$, whence the n elements $bs_1, \ldots, bs_n$ are distinct and therefore constitute all of S. Hence $bx = s$ is solvable for every $s \in S$, whence b is a universal left divisor of S.

Proof of sufficiency. If b is a universal left divisor of S, *i.e.*, if the equation $bx = s$ is solvable for every $s \in S$, then there are in S exactly n distinct elements $bx_1, \ldots, bx_n$, where n is the order of S, and $i \neq j$ implies $x_i \neq x_j$. Hence the elements $x_1, \ldots, x_n$ constitute all of S, whence $bx = by$ implies $x = y$ for any $x, y \in S$, *i.e.*, b is left cancellable in S.

Theorem 2.6. *The right divisors of a left identity element of a finite semigroup S form a subgroup of the semigroup of left cancellable elements of S.*

Proof. Let e be any left identity element of S. By Theorem 2.3, the right divisors of e form a subsemigroup of the semigroup of left cancellable elements of S.

But in a finite semigroup, by Lemma 2.2, the left cancellable elements coincide with the universal left divisors; and, by Lemma 2.1, each universal left divisor in a finite semigroup generates a cyclic group. Hence each right divisor of e generates a cyclic group. Since the right divisors of e form a semigroup, any positive integral power of a right divisor of e is also a right divisor of e, whence all elements lying in the cyclic groups generated by right divisors of e are right divisors of e. Hence if r is any right divisor of e and k is any positive integer then $e = yr^k$ for some $y \in S$. Now if i is the identity element of the cyclic group generated by r, we have $e = yr^k = y(r^k i) = (yr^k)i = ei = i$, whence e is a common identity element for all the cyclic groups generated by right divisors of e. Now let R_e be the set of all right divisors $r_1, \ldots, r_m$ of e, and let $R_1, \ldots, R_m$ be the respective cyclic groups generated by these right divisors. Then $R_e = R_1 \cup \cdots \cup R_m$. Let $a, b \in R_e$; then $a \in R_j$ $(1 \leq j \leq m)$, and we may denote by a^{-1} the inverse of a in the group R_j. Now $a(a^{-1}b) = (aa^{-1})b = eb = b$, and $a^{-1}b \in R_e$ since R_e is a semigroup. Hence $ax = b$ is solvable in R_e for arbitrary $a, b \in R_e$. And $(ba^{-1})a = b(a^{-1}a) = be = b$, the last equality arising from the fact that $b \in R_k$ $(1 \leq k \leq m)$ and e is the identity element of R_k; hence the equation

$ya = b$ is solvable in R_e . Therefore R_e is a group, as was to be proved.

We note that an example may be given (the direct product[19] of Nos. 2.1 and 4.57) to show that the right divisors of a left identity element need not all generate the same cyclic group. We note also that in a finite semigroup the left divisors of a left identity element (= universal left divisors = left cancellable elements) need not form a group; example: No. 4.65. In fact, we have

Theorem 2.7. _If the left divisors of a left identity element_ e _of a finite semigroup_ S _form a group, then_ e _is the only left identity element of_ S .

Proof. By Theorem 2.2, all left identity elements of S have a common set D of left divisors. But every left identity element lies in D , and each such element is idempotent. Since a group can contain only one idempotent element, there can be only one left identity element e in S , and it is the identity element of the group of left divisors of e .

By left-right duality the foregoing theorems yield

Theorem 2.8. _In a finite semigroup_ S _with a two-sided identity element_ e , _the left divisors of_ e , _right divisors of_ e , _left cancellable elements, and right cancellable elements_

---

[19] The multiplication table of this semigroup may be found in Harden, _op. cit._, p. 20.

all coincide and constitute a subgroup of S.

3. Divisors of zero.

Theorem 3.1. *The left divisors of a right zero element of a semigroup* S *form a left ideal of* S.

Proof. Let z be a right zero element of S, let $dx = z$, and let $s \in S$. Then $(sd)x = s(dx) = sz = z$, whence sd is a left divisor of z. Hence if D is the set of all left divisors of z we have $SD \subseteq D$, *i.e.*, D is a left ideal of S.

We note that the left divisors of a left zero element of S need not form an ideal, nor even a subsemigroup, of S. For example, in No. 4.63 the element 2 is a left zero element, and its left divisors are 2, 3, and 4; but $4 \cdot 2 = 1$.

Theorem 3.2. *If a semigroup* S *has a two-sided zero element* z, *then the left divisors of* z *form a left ideal of* S, *the right divisors of* z *form a right ideal of* S, *and the two-sided divisors of* z *form a subsemigroup of* S.

Proof. The first two statements are immediate from Theorem 3.1 and its left-right dual. Let L be the left ideal of left divisors of z and R the right ideal of right divisors of z. Then the set of all two-sided divisors of z is the intersection $L \cap R$. But any left or right ideal of S is a subsemigroup of S, and the intersection of subsemigroups, if non-empty, is a subsemigroup.

Now $L \cap R \neq \emptyset$ since $z \in L \cap R$, whence $L \cap R$ is a subsemigroup of S .

We observe that the semigroup of two-sided divisors of a two-sided zero element need not be a two-sided ideal of S . An example may be extracted from the transformation semigroup of degree four (= semigroup of all single-valued mappings of a set of four objects into itself), the multiplication table of which has been given in full by Posey;[20] in Posey's notation, the exemplary subsemigroup consists of the mappings A_1, A_7, B_2, B_8, B_{27}, B_{47}, B_{55}, B_{115}, B_{121}, C_1, C_4, C_{27}, C_{33}, C_{34}, C_{55}, C_{61}, and D_1 .

Among the divisors of a two-sided zero element are the nilpotent elements. In a commutative semigroup S these form a subsemigroup, for if $a, b \in S$ and $a^m = a^n = z$, where z is a two-sided zero element of S , then $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = z \cdot z = z$. In a non-commutative semigroup, however, this need not be the case. For example, in the semigroup whose multiplication table is exhibited below the element 1 is a two-sided zero element and 2 and 3 are nilpotent, but $(2 \cdot 3)^2 = 4^2 = 4$.

---

[20]E. E. Posey, Endomorphisms and Translations of Semigroups, University of Tennessee Master's Thesis, 1949.

	1	2	3	4	5
1	1	1	1	1	1
2	1	1	4	1	2
3	1	5	1	3	1
4	1	2	1	4	1
5	1	1	3	1	5

We may find an example in the multiplicative semigroup of all second-order square matrices over the ring of integers to show that the left divisors of a nilpotent element need not form a semigroup. Let

$$N = \begin{pmatrix} -10 & -20 \\ 5 & 10 \end{pmatrix}, \quad A = \begin{pmatrix} 5 & 5 \\ 1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} -2 & 4 \\ 1 & -2 \end{pmatrix}.$$

Then N is nilpotent, and A and B are left divisors of N since

$$\begin{pmatrix} 5 & 5 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} -9 & -18 \\ 7 & 14 \end{pmatrix} = \begin{pmatrix} -10 & -20 \\ 5 & 10 \end{pmatrix} = \begin{pmatrix} -2 & 4 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 7 & 12 \\ 1 & 1 \end{pmatrix}.$$

But $AB = \begin{pmatrix} -5 & 10 \\ 0 & 0 \end{pmatrix}$, whence AB cannot be a left divisor of N, for if X is any matrix then the second row of ABX must consist entirely of zeros.

4. Union, intersection, product, and direct product of prime ideals.

Definition 4.1. A left (right, two-sided) ideal P of a semigroup S is said to be prime if $a, b \in S$ and $ab \in P$ jointly imply that either $a \in P$ or $b \in P$. Clearly, a prime ideal might be defined equivalently as an ideal whose complement is either empty (in case the ideal is S itself, which is obviously prime) or a subsemigroup of S . It is also clear that a left (right, two-sided) zero element of S is a prime right (left, two-sided) ideal of S if and only if it has no proper divisors.

Theorem 4.1. The union of an arbitrary collection of prime right ideals of a semigroup S is a prime right ideal of S .

Proof. Let $[R_\iota]$ be a collection of prime right ideals of S , where ι ranges over an index set M of arbitrary cardinality. Then if a, b $\in$ S and ab $\in \bigcup_{\iota \in M} P_\iota$ we must have ab $\in P_\iota$ for some $\iota \in M$. But P_ι is prime, whence either a $\in P_\iota$ or b $\in P_\iota$. Therefore either a $\in \bigcup P_\iota$ or b $\in \bigcup P_\iota$, whence $\bigcup P_\iota$ is prime. Similarly for left and two-sided prime ideals.

The union of two or more ideals may be prime, however, even though none of the given ideals be prime; for example, in No. 4.66 each of the elements 1 and 2 is a left zero element and hence a right ideal, and neither is prime since $3 \cdot 2 = 1$ and $4 \cdot 1 = 2$; but their union is prime.

We now raise the question whether the product of two or more prime right ideals need be prime. Without further hypotheses, the answer is negative, for in No. 4.71 the right ideals [1, 3, 4] and [4] are prime, while their product [1, 4] is not. On the other hand, in No. 4.67 the product [3, 4] of the prime right ideals [2, 3, 4] and [4] is also prime. We observe that in both these examples one of the factors is properly contained in the product, and we find that when this situation does not obtain we can find necessary and sufficient conditions that a product of prime right ideals be prime.

<u>Theorem 4.2</u>. <u>If a product of a finite set of prime right ideals of a semigroup S is prime, then the product ideal contains at least one of the given ideals</u>.

<u>Proof</u>. Let $R_1, \ldots, R_n$ be prime right ideals of S, and let $\prod_j^k R_i$ be an abbreviation for the product $R_k R_{k+1} \cdots R_n$ $(1 \leq k \leq n)$. We wish to prove that if $\prod_1^n R_i$ is prime then $R_k \subseteq \prod_1^n R_i$ for some k $(1 \leq k \leq n)$. Suppose, to the contrary, that $R_k \not\subseteq \prod_1^n R_i$ for all $k = 1, \ldots, n$. Then for each k there is an element $a_k \in R_k$ such that $a_k \notin \prod_1^n R_i$. Now $a_1 \cdot \prod_2^n a_i = \prod_1^n a_i \in \prod_1^n R_i$, whence $\prod_2^n a_i \in \prod_1^n R_i$ since $a_1 \notin \prod_1^n R_i$ and $\prod_1^n R_i$ is prime. Now if we make the inductive assumption that $a_k \cdot \prod_{k+1}^n a_i = \prod_k^n a_i \in \prod_1^n R_i$, then since $a_k \notin \prod_1^n R_i$ we have $\prod_{k+1}^n a_i \in \prod_1^n R_i$. Hence by complete induction we conclude that $a_n \in \prod_1^n R_i$, contrary to our choice of a_n, and the theorem is proved.

We have already cited an example (No. 4.71) which shows that the converse statement "if a product of prime right ideals contains one of them then the product is prime" is false. However, we may state Theorem 4.2 in a slightly different form, and combine it with the trivial observation that if the product of prime ideals is one of those ideals then the product is prime, to obtain

Theorem 4.3. _If a product of prime right ideals of a semigroup does not properly contain any of them, then the product is prime if and only if it is one of the given ideals._

The proof of Theorem 4.2 holds _mutatis mutandis_ for two-sided ideals, and for these we may drop the hypothesis concerning proper inclusion in Theorem 4.3. For, as we have already noted (in (4) of Definition 1.8), any product of two-sided ideals is contained in their intersection, so that the product cannot contain any of them properly and the inclusion hypothesis in Theorem 4.3 is satisfied automatically. Hence we have

Theorem 4.4. _A product of prime two-sided ideals of a semigroup is prime if and only if it is one of the given ideals._

Corollary. _If a product of prime two-sided ideals of a semigroup is prime, then the product of the ideals is just their intersection._

The converse of this corollary fails, however, because the intersection of the ideals may be a proper subset of each of them. For example, in the commutative semigroup No. 4.23 the ideal [1, 4] is both the product and the intersection of the prime ideals [1, 2, 4] and [1, 3, 4], but is not prime.

The intersection of prime right ideals need not be prime; for example, in No. 4.66 the prime right ideals $[1, 2]$ and $[1, 3]$ intersect in the right ideal $[1]$, which is not prime. However, the question whether the non-empty intersection of a set of prime right ideals of a semigroup S is prime in S may be reduced to the question whether the intersection is prime in the union of the given ideals.

Theorem 4.5. The intersection of a set of prime right ideals of a semigroup S is a prime right ideal of S if and only if it is a prime right ideal of the union of the given ideals.

Proof. The necessity being obvious, we proceed to prove the sufficiency. Let $[R_\iota]$ be a set of prime right ideals of S, where ι ranges over an arbitrary index set M. By hypothesis, $\bigcap_{\iota \in M} R_\iota$ is a prime right ideal of $\bigcup_{\iota \in M} R_\iota$ and hence is non-empty. Let $x, y \in S$, $xy \in \bigcap_{\iota \in M} R_\iota$. Then if $x \notin \bigcap_{\iota \in M} R_\iota$ there is some R_λ $(\lambda \in M)$ such that $x \notin R_\lambda$; and if $y \notin \bigcap_{\iota \in M} R_\iota$ then there is some R_μ $(\mu \in M)$ such that $y \notin R_\mu$. Hence $x, y \notin R_\lambda \cap R_\mu$. But $xy \in \bigcap_{\iota \in M} R_\iota \subseteq R_\lambda \cap R_\mu$, and both R_λ and R_μ are prime, whence either $x \in R_\lambda$ or $y \in R_\lambda$, and either $x \in R_\mu$ or $y \in R_\mu$. Therefore, we have either $x \in R_\lambda$ and $y \in R_\mu$ or else $y \in R_\lambda$ and $x \in R_\mu$. In either case, $x, y \in R_\lambda \cup R_\mu \subseteq \bigcup_{\iota \in M} R_\iota$. But, by hypothesis, $\bigcap_{\iota \in M} R_\iota$ is prime in $\bigcup_{\iota \in M} R_\iota$, whence either $x \in \bigcap_{\iota \in M} R_\iota$ or $y \in \bigcap_{\iota \in M} R_\iota$. Hence $\bigcap_{\iota \in M} R_\iota$ is a prime ideal of S.

Clearly the foregoing theorem is equally valid for two-sided ideals, but for finite sets of these we have the following more specific result.

Theorem 4.6. The intersection of a finite set of prime two-sided ideals of a semigroup S is prime if and only if the intersection is one of the given ideals.

Proof. The sufficiency is trivial. To prove the necessity, let $A_1, \ldots, A_n$ be prime two-sided ideals of S, and recall that their intersection must be non-empty. If $\bigcap_1^n A_i \neq A_k$ for all $k = 1, \ldots, n$, then for each k there is an element $a_k \in A_k$ such that $a_k \notin \bigcap_1^n A_i$. Now, exactly as in the proof of Theorem 4.2, we may prove inductively that if $\prod_1^n a_i \in \bigcap_1^n A_i$ then $a_n \in \bigcap_1^n A_i$, contrary to the choice of a_n, and hence conclude that $\prod_1^n a_i \notin \bigcap_1^n A_i$. But $\prod_1^n a_i \in \prod_1^n A_i \subseteq \bigcap_1^n A_i$. Hence the supposition that $\bigcap_1^n A_i \neq A_k$ for all $k = 1, \ldots, n$ is contradicted, and our theorem is proved.

Definition 4.2. The direct product of two semigroups S and T is defined to be a system whose elements are all the ordered pairs (s, t), with $s \in S$ and $t \in T$, and with multiplication defined by $(s_1, t_1)(s_2, t_2) = (s_1s_2, t_1t_2)$. The definition may be extended readily to the direct product of any finite set of semigroups. It is well known (and easily proved) that a direct product of semigroups is a semigroup,[21]

[21]Harden, op. cit., p. 5.

and that a subset of such a direct product is a left (right, two-sided) ideal thereof if and only if the subset is the direct product of left (right, two-sided) ideals of the factors.[22]

Our purpose in introducing direct multiplication at this point is simply to point out that the direct product of prime ideals of two semigroups need not be prime in the direct product of the semigroups. For example, the commutative semigroups No. 2.2 and No. 3.16 each have a zero element, and the ordered pair of zero elements is (necessarily) a zero element of the direct product,[23] and hence a two-sided ideal; but it has proper divisors and therefore is not prime.

5. Prime ideals in semigroups with identity elements.

In this section and the next we shall be concerned with maximal ideals as well as with prime ideals, and a few words concerning the property of maximality seem to be in order here.

We note first that while a two-sided ideal which is a maximal right ideal is necessarily a maximal two-sided ideal, the converse need not hold. For example, in No. 4.74 the ideal [3, 4] is a maximal two-sided ideal but is properly contained in the proper maximal right ideals [1, 3, 4] and [2, 3, 4].

---

[22] *Ibid.*, p. 7.

[23] *Ibid.*, p. 15, the multiplication table is given.

A similar situation arises whenever we discuss maximality with respect to the conjunction of two or more properties. In particular, under Definition 1.9 a maximal prime right ideal of a semigroup S is a prime right ideal which is not properly contained in any proper prime right ideal of S . Such an ideal need not be a maximal right ideal of S ; for example, in No. 4.25 the maximal prime two-sided ideal [4] is properly contained in the proper two-sided ideal [1, 2, 4] . To avoid ambiguity, we might speak of a maximal prime right ideal as <u>maximal among the prime right ideals</u> of S , and similarly for left and two-sided ideals. On the other hand, a <u>prime maximal right (left, two-sided) ideal</u> is a maximal right (left, two-sided) ideal of S which is also a prime ideal of S ; this concept will recur frequently in the sequel.

We shall have occasion to use repeatedly the obvious fact that if a left (right, two-sided) ideal A of S contains every proper left (right, two-sided) ideal of S , then A is an unique maximal left (right, two-sided) ideal of S .

We note in passing that maximality of ideals (even of prime ideals) is not preserved under direct multiplication. For example, in the direct product[24] of Nos. 2.2 and 3.16 the zero element is not a maximal ideal, although the zero

---

[24] *Ibid.*, p. 14.

elements of the respective factors are both maximal and prime.

Definition 5.1. We extend Definition 1.5 by introducing a new kind of divisor. If $a, b \in S$ we shall say that a is an *internal divisor* of b if there exist elements $x, y \in S$ such that $xay = b$. An element which is not a left (right, internal) divisor of b may be called a *left* (*right*, *internal*) *non-divisor* of b.

Theorem 5.1. The set of all right non-divisors of an arbitrary element b *of a semigroup* S *either is empty (in which case* b *is a left zeroid element of* S *and hence*[25] *lies in the intersection of all left ideals of* S *) or else is a left ideal of* S *; and dually. The set of all internal non-divisors of* b *either is empty or is a two-sided ideal of* S.

Proof. Let a be a right non-divisor of b and let $x \in S$. Then if sa is a right divisor of b, *i.e.*, if $x(sa) = b$ for some $x \in S$, we have $(xs)a = b$, contrary to the hypothesis that a is a right non-divisor of b. Hence sa is a right non-divisor of b for every $s \in S$ and every right non-divisor a; *i.e.*, the right non-divisors form a left ideal of S.

Now let a be an internal non-divisor of b, and let $s \in S$. Then if sa is an internal divisor of b we have $b = x(sa)y = (xs)ay$ for some $x, y \in S$; and if as is an

[25]Clifford and Miller, *op. cit.*, p. 118.

internal divisor of b we have $b = u(as)v = ua(sv)$ for some $u, v \in S$. In each case the hypothesis that a is an internal non-divisor of b is contradicted. Therefore sa and as are internal non-divisors of b, whence the internal non-divisors of b constitute a two-sided ideal of S.

It may be noted that when an element b has at least one right (left, internal) non-divisor, the left (right, two-sided) ideal of all such non-divisors need not be prime; for example, in No. 4.69 the right divisors of 2 do not form a semigroup, whence the left ideal of right non-divisors of 2 is not prime. It may also be remarked that the right non-divisors of b, when they exist, need not form a right ideal of S; for example, in No. 4.84 the only right non-divisor of 1 is 4, which is a right zero element, and hence a left ideal, but is not a right ideal.

Lemma 5.1. *If a right ideal A of a semigroup S contains a left divisor of a left identity element e of S, then $A = S$; and dually. If a two-sided ideal M of S contains an internal divisor of e, then $M = S$.*

Proof. If $a \in A$ and $ax = e$ for some $x \in S$, then $e = ax \in AS \subseteq A$, whence $S = eS \subseteq AS \subseteq A$, so that $A = S$. If $m \in M$ and $xmy = e$ for some $x, y \in S$, then $e = xmy \in SMS \subseteq M$, whence $S = S(eS) = SeS \subseteq SMS \subseteq M$, so that $M = S$.

Throughout the rest of this section, we shall be concerned with non-divisors of one-sided and two-sided identity elements. To avoid tiresome repetition, we prescribe the following notation for the remaining developments of this section: in a semigroup S with left, right, or two-sided identity element e, L will denote the set of all right non-divisors of e, R the set of all left non-divisors of e, and T the set of all internal non-divisors of e. It should be noted that L, R, and T are proper subsets of S; for $eee = ee = e$, whence e has at least one internal divisor, at least one right divisor, and at least one left divisor. We shall use this fact repeatedly without further explicit mention of it in the proofs.

Theorem 5.2. *In a semigroup S containing a left identity element e, if $R \neq \emptyset$ then R is an unique proper maximal right ideal of S, and is prime.*

Proof. By Theorem 5.1, R is a right ideal of S. If A is any right ideal of S, and $A \not\subseteq R$, then, since R is the set of all left non-divisors of e, there is an element $a \in A$ such that $ax = e$ for some $x \in S$. Hence, by Lemma 5.1, $A = S$. Therefore R contains every proper right ideal of S and hence is an unique maximal right ideal of S. By Theorem 2.1, $C(R)$ is a semigroup, whence R is a prime ideal.

Corollary. If a semigroup S contains a left identity element e and contains a proper right ideal A, then S contains an unique proper maximal right ideal, which is prime.

Proof. Since A is proper by hypothesis, it follows from Lemma 5.1 that A contains no left divisor of e. Hence $A \subseteq R$, whence $R \neq \emptyset$ and Theorem 5.2 yields the desired conclusion.

Theorem 5.3. *In a semigroup S containing a left identity element e, if $L \neq \emptyset$ then L is a proper prime left ideal of S; if S is finite, L is a maximal left ideal of S.*

Proof. By Theorem 5.1, L is a left ideal of S, and by Theorem 2.1 it is prime. If S is finite, suppose $L \subset B \subseteq S$, where B is a left ideal of S. Then, since L is the set of all right non-divisors of e, there is an element $b \in B$ such that $yb = e$ for some $y \in S$, whence $e = yb \in SB \subseteq B$. But, by Theorem 2.6, $C(L)$ is a group with e as its identity element, whence $C(L) \circ e = C(L)$. Hence $C(L) = C(L) \circ e \subseteq C(L) \circ B \subseteq SB \subseteq B$, whence $L \cup C(L) \subseteq B$. But $L \cup C(L) = S$, whence $B = S$. Therefore L is a proper maximal left ideal of S.

We note that the proper maximal ideal L, unlike R, need not be unique; see, for example, No. 4.57.

Theorem 5.4. *In a semigroup S containing a left identity element e, if $T \neq \emptyset$ then T is an unique proper maximal two-sided ideal of S.*

Proof. Let $T \neq \emptyset$ and let M be any proper two-sided ideal of S. If $M \nsubseteq T$ then M contains at least one internal divisor of e, whence, by Lemma 5.1, $M = S$. Thus T contains every proper two-sided ideal of S, whence T is an unique proper maximal two-sided ideal of S.

Corollary. If a semigroup S contains a left identity element e and a proper two-sided ideal M, then S contains an unique proper maximal two-sided ideal.

Proof. By Lemma 5.1, M contains no proper internal divisor of e, whence $M \subseteq T$, $T \neq \emptyset$, and Theorem 5.4 applies.

Theorem 5.5. In a semigroup S containing a left identity element e, $L = \emptyset$ if and only if S is a group; if S is a group then $R = T = \emptyset$; $T \subseteq R$, and if S is finite then $T = R \subseteq L$.

Proof. If S is a group, then S contains no proper left or right or two-sided ideals; hence $L = R = T = \emptyset$. If $L = \emptyset$ then every element of S is a right divisor of e, *i.e.*, every element has a left inverse with respect to the left identity element e, whence S is a group. If $t \in T$ and $tx = e$ for some $x \in S$ then $etx = (et)x = tx = e$, whence $t \notin T$; hence if $t \in T$ then $tx \neq e$ for all $x \in S$, *i.e.*, $T \subseteq R$. If S is finite then, by Lemma 2.2 and Theorem 2.6, $R \subseteq L$, whence if $R = \emptyset$ then $T = R = \emptyset$. And if $R \neq \emptyset$ (still assuming

S to be finite) let $a \in R$; then, if $xay = e$ for some $x, y \in S$, we have $ay \in C(L) \subseteq C(R)$, i.e., ay is a left divisor of e , whence a is a left divisor of e , contrary to the hypothesis that $a \in R$. Therefore if S is finite then $R \subseteq T$, so that $T = R \subseteq L$.

We may now classify semigroups containing left identity elements according to the emptiness or non-emptiness of the sets L , R , and T . Although à priori eight cases could arise, it follows from the relations exhibited in Theorem 5.5 that only four of these can arise: (1) $L = R = T = \emptyset$, S being a group in this case and only in this case; (2) $L \neq \emptyset$, $R = T = \emptyset$, No. 4.65 being an example of this case; (3) $L \neq \emptyset$, $R \neq \emptyset$, $T \neq \emptyset$, No. 4.60 being an example of this case; (4) $L \neq \emptyset$, $R \neq \emptyset$, $T = \emptyset$, there being no finite example of this case according to Theorem 5.5. We have not found an example of Case (4), but we can give an example to show that if S is infinite we may have $T \neq R$. Let S be the semigroup of all single-valued mappings of the set N of non-negative integers into itself, let ι denote the identity mapping $n \rightarrow n$ (a two-sided identity element of S), and for any elements $\varphi, \psi \in S$ define $\varphi\psi$ to be the result of performing first ψ , then φ . Now let φ be defined by $\varphi(n) = n + 1$ for even integers n and $\varphi(n) = n$ for odd n . Since $\varphi(N) \neq N$, φ cannot be a left divisor of ι . Let ψ be defined by $\varphi(n) = 2n$ for all $n \in N$, and let χ be defined by $(n) = 0$ for even n and $\chi(n) = (1/2)(n-1)$ for odd n. Then $\chi\varphi\psi(n) = n$ for all $n \in N$, whence $\chi\varphi\psi = \iota$. Therefore $\varphi \in R$ while $\varphi \notin T$.

These findings, together with Theorem 2.2, may be summarized in

Theorem 5.6. *If a semigroup S containing a left identity element is not a group, then S contains at least one proper prime left ideal, and, unless every element of S is a left divisor of all elements of S, contains an unique proper maximal right ideal. If S is finite, and is not a group, it contains a proper maximal left ideal, and its proper maximal right ideal, if it exists, is also an unique maximal two-sided ideal.*

For semigroups having two-sided identity elements, we may combine the foregoing theorems with their left-right duals to obtain

Theorem 5.7. *In a semigroup S having a two-sided identity element, if S is not a group then S contains proper maximal left and right ideals, each unique and prime, and an unique maximal two-sided ideal which is prime if S is finite.*

We can improve upon the last part of Theorem 5.7 by proving

Theorem 5.8. *If T is the maximal proper two-sided ideal of a semigroup S with two-sided identity element e, and if*

<u>$C(T)$ is finite, then T is a prime ideal and $C(T)$ is a group.</u>

<u>Proof.</u> Let A be the set of all left divisors of e, B the set of all right divisors of e, and D the set of all internal divisors of e. Then $C(T) = D$ and $A \cup B \subseteq D$. By Theorem 2.3 and its dual, A and B are finite semigroups; and each element of A is a left divisor of the right identity element e, and each element of B a right divisor of the left identity element e. Hence, by Theorem 2.6 and its dual, A and B are groups. Therefore, for arbitrary $a \in A$, there exists an element $a^{-1} \in A$ such that $a^{-1} a = e$, so that a is a right divisor of e and hence $A \subseteq B$. Similarly, $B \subseteq A$, whence $A = B$. Now let $d \in D$; then $xdy = e$ for some $x, y \in S$, and necessarily $x, y \in C(T)$ since x is a left and y a right divisor of e. Hence $xd \in A = B$, whence xd, and therefore d, is a right divisor of e. Therefore $D \subseteq B$, whence $D = A = B$, $C(T)$ is a group, and T is prime.

The proof just completed shows that the set D of all divisors of a two-sided identity element of a semigroup is a group if D is finite. A familiar example is the group $[\pm 1, \pm i]$ in the semigroup of Gaussian integers.

<u>6. Prime ideals and maximal ideals.</u>

In this concluding section we investigate the conditions under which a maximal ideal is prime, without assuming the existence of an identity element.

Theorem 6.1. *If M is a maximal two-sided ideal of a semigroup S, and if the complement of M is commutative and is contained in S^2, then M is a prime ideal of S.*

Proof. The theorem is trivial if $M = S$. Let M be a proper maximal ideal and suppose M is not prime; then there exist elements x and y (not necessarily distinct) in $C(M)$ such that $xy \in M$. Let x be some fixed element of $C(M)$ such that, for at least one element $y \in C(M)$, $xy \in M$, and let Y be the set of all such elements y. We distinguish two cases: (1) $Y \subset C(M)$ and (2) $Y = C(M)$.

Case (1): In this case we shall show that $M \cup Y$ is a two-sided ideal of S, *i.e.*, that $(M \cup Y)S \subseteq M \cup Y$ and $S(M \cup Y) \subseteq M \cup Y$. Since $S = M \cup C(M)$, we may accomplish this by showing that $(M \cup Y)M \subseteq M \cup Y$ and $M(M \cup Y) \subseteq M \cup Y$, which is obvious since M is a two-sided ideal, and that $(M \cup Y)\circ C(M) \subseteq M \cup Y$ and $C(M)\circ(M \cup Y) \subseteq M \cup Y$. Now if $y \in Y$ and $c \in C(M)$ then $x(yc) = (xy)c \in M$, for $xy \in M$; hence either $yc \in M$ or $yc \in Y$, so that $(M \cup Y)\circ C(M) \subseteq M \cup Y$. And since we have assumed $C(M)$ to be commutative, $x(cy) = x(yc) = (xy)c \in M$, whence either $cy \in M$ or $cy \in Y$, and therefore $C(M)\circ(M \cup Y) \subseteq M \cup Y$. This completes the proof that $M \cup Y$ is a two-sided ideal. Since Y is non-empty and $M \cap Y = \emptyset$, $M \subset M \cup Y$;

and $M \cup Y \subset S$ since in this case we have assumed $Y \subset C(M)$. Therefore $M \cup Y$ is a proper two-sided ideal of S, properly containing M, contrary to the hypothesis that M is maximal.

Case (2): If $Y = C(M)$ then, by virtue of the hypothesis that $C(M)$ is commutative, $yx = xy \in M$ for all $y \in C(M)$, whence $xS \subseteq M$ and $Sx \subseteq M$. In particular, $x^2 \in M$, whence $x \neq x^2$. But since $C(M) \subseteq S^2$, there exist elements a and b (not necessarily distinct) in S such that $x = ab$; and both a and b lie in $C(M)$ since $x \in C(M)$. Now either $a \neq x$ or $b \neq x$, for if $a = b = x$ then $x = ab = x^2$; say $a \neq x$. Hence $M \cup x$ is a two-sided ideal of S, for $(M \cup x)S = MS \cup xS \subseteq M \cup M \subseteq M \subseteq M \cup x$ and $S(M \cup x) = SM \cup Sx \subseteq M \cup M \subseteq M \subseteq M \cup x$. But $M \subset M \cup x$ since $x \in C(M)$; and $M \cup x \subset S$ since $a \in C(M)$ and $a \neq x$. Therefore $M \cup x$ is a proper two-sided ideal of S, properly containing M, contrary to the hypothesis that M is maximal.

The supposition that M is not prime having led to a contradiction in both cases, we conclude that M is prime.

We observe that in the above proof of Case (1) no use was made of the hypothesis that $C(M) \subseteq S^2$. Hence by combining the maximality of M, the commutativity of $C(M)$, and the condition defining Case (1), we obtain the

Corollary 1. *If* M *is a maximal two-sided ideal of a semigroup, if the complement* $C(M)$ *is commutative, and if, for every element* $x \in C(M)$, $x \circ C(M) \not\subseteq M$, *then* M *is a prime ideal.*

The condition $x \circ C(M) \not\subseteq M$ which suffices in the presence of the maximality of M and the commutativity of the complement may be contrasted with the much stronger defining condition for prime ideals, *viz.*, $[C(M)]^2 \subseteq C(M)$.

An immediate consequence of Theorem 6.1 is

Corollary 2. *In a semigroup* S *such that* $S^2 = S$, *every maximal two-sided ideal whose complement is commutative is prime. In particular, in a semigroup having either a left or a right identity element every maximal two-sided ideal whose complement is commutative is prime. In a commutative semigroup such that* $S^2 = S$ (*and à fortiori in a commutative semigroup with identity*), *every maximal ideal is prime.*

We now prove a converse of Theorem 6.1, and are able to drop the hypothesis that the complement of the ideal be commutative.

Theorem 6.2. *If* M *is a maximal and prime two-sided ideal of a semigroup* S , *then the complement of* M *is contained in* S^2 .

Proof. Suppose $C(M) \not\subseteq S^2$, and let x be any element of $C(M)$ such that $x \notin S^2$. Then $x \neq x^2$, and $x^2 \in C(M)$ since M is prime. Now the set

$M \cup x^2 \cup Sx^2 \cup x^2S \cup Sx^2S$ is a two-sided ideal of S ; for $MS \subseteq M$, $SM \subseteq M$, $S(Sx^2) = S^2x^2 \subseteq Sx^2$, $(x^2S)S = x^2S^2 \subseteq x^2S$, $(Sx^2)S = S(x^2S) = Sx^2S$, $S(Sx^2S) = S^2x^2S \subseteq Sx^2S$, and $(Sx^2S)S = Sx^2S^2 \subseteq Sx^2S$. But $M \subset (M \cup x^2 \cup Sx^2 \cup x^2S \cup Sx^2S)$ since $x^2 \notin M$; and $(M \cup x^2 \cup Sx^2 \cup x^2S \cup Sx^2S) \subset S$ since $x \notin M$ and $x \notin S^2$. Therefore $M \cup x^2 \cup Sx^2 \cup x^2S \cup Sx^2S$ is a proper two-sided ideal of S properly containing M , contrary to the hypothesis that M is maximal.

We note in passing that if A is any left or right ideal of a semigroup S , and if $C(A) \subseteq S^2$, then $C(A) \subset S^2$; for S^2 is a two-sided ideal of S , whence $S^2 \cap A \neq \emptyset$ while $C(A) \cap A = \emptyset$, and so $C(A) \neq S^2$. Hence the conclusion of Theorem 6.2 could be strengthened to read "the complement of M is contained properly in S^2 ". We note also that, in any semigroup S , the ideal S^2 is prime if and only if $S^2 = S$; and that S^2 is maximal if and only if $C(S^2)$ contains at most a single element, the "only if" following from the fact that if $x, y \in C(S^2)$ and $x \neq y$ then $S^2 \cup x$ is a proper ideal of S properly containing S^2 .

Theorems 6.1 and 6.2 together yield

<u>Theorem 6.3. In a semigroup</u> S , <u>a maximal two-sided ideal whose complement is commutative is a prime ideal if and only if the complement is contained in</u> S^2 .

It is a well-known theorem[26] in the theory of rings that if M is an ideal in a commutative ring R then the residue class ring R/M is a field if and only if both (1) M is a maximal ideal of R and (2) $x^2 \in M$ implies $x \in M$. Another familiar result is the theorem[27] that an ideal in a commutative ring R is a prime ideal of R if and only if R/M is an integral domain. Since every field is an integral domain (but not conversely), it follows that if conditions (1) and (2) hold then M is a prime ideal; the converse fails because, although every prime ideal satisfies condition (2), a prime ideal need not be maximal. However, it follows that if M is a maximal ideal in a commutative ring then M is prime if and only if (2) holds, and this result we shall prove both for one-sided and for two-sided ideals in semigroups, dispensing with the hypothesis of commutativity. Before preceeding to the proofs, we remark that it is easy to show[28] that in a commutative ring with identity element condition (2) follows from condition (1), whence we conclude that in such a ring every maximal ideal is prime. This result carries over to commutative semigroups with identity, as we have seen in Corollary 2 to Theorem 6.1;

---

[26]Neal H. McCoy, Rings and Ideals (Buffalo: Math. Assn. of Amer., 1948), pp. 80-81.

[27]Ibid., p. 98.

[28]Ibid., p. 81.

indeed, we have seen (loc. cit.) that in any semigroup with identity a maximal ideal whose complement is commutative must be prime. The commutativity cannot be dropped altogether however, unless some such condition as finiteness be substituted for it, as in Theorem 5.8. We shall give an example later to show that in an infinite semigroup with two-sided identity element a maximal two-sided ideal need not be prime.

We now state and prove the theorems announced in the foregoing paragraph, giving separate proofs for one-sided and two-sided ideals; neither proof seems readily adaptable to the other theorem.

Theorem 6.4. *A maximal right ideal M of a semigroup S is a prime right ideal of S if and only if $x^2 \in M$ implies $x \in M$.*

Proof. The necessity of the condition follows immediately from the definition of prime ideal. To prove the sufficiency, suppose that M is not prime. Then there exist elements x and y lying in the complement of M such that $xy \in M$. Since $x^2 \in M$ implies $x \in M$ by hypothesis, $x \neq y$ and $x^2, y^2 \in C(M)$. Now $x \notin yS$; for if $x = ys$ for some $s \in S$ then $(xy)s = x(ys) = x^2 \in C(M)$, contrary to our supposition that xy lies in the right ideal M. Hence we have $x \notin M$, $x \neq y$, and $x \notin yS$, whence $x \notin (M \cup y \cup yS)$ and therefore $(M \cup y \cup yS) \subset S$. And $M \subset (M \cup y \cup yS)$, for $y \notin M$. But the set

$M \cup y \cup yS$ is a right ideal of S, for

$$(M \cup y \cup yS)S = MS \cup yS \cup yS^2 \subseteq M \cup y \cup yS .$$

Therefore $M \cup y \cup yS$ is a proper right ideal of S, properly containing M, contrary to the hypothesis that M is a maximal right ideal of S.

In the case of two-sided ideals, the above proof breaks down because, although a two-sided ideal is a right ideal, a maximal two-sided ideal need not be a maximal right ideal, *i.e.*, a two-sided ideal may be contained properly in a proper right ideal even though it is not a proper subset of any proper two-sided ideal. For example, in No. 4.67 the proper two-sided ideal [3, 4] is maximal, but is properly contained in the proper right ideals [1, 3, 4] and [2, 3, 4] .

Lemma 6.1. If M *is a two-sided ideal of a semigroup* S*, and if* $x^2 \in M$ *implies* $x \in M$*, then* $xy \in M$ *implies* $yx \in M$*; if* $x \in S$*, if* Y *is the set of all elements* $y \in S$ *such that* $xy \in M$*, and if* Z *is the set of all elements* $z \in S$ *such that* $zx \in M$*, then* $Y = Z$.

Proof. If $xy \in M$ then $(yx)^2 = (yx)(yx) = y(xy)x \in M$, whence $yx \in M$. Hence if $y \in Y$ then $y \in Z$, and vice-versâ, so that $Y = Z$.

Theorem 6.5. A maximal two-sided ideal M *of a semigroup* S *is a prime ideal of* S *if and only if* $x^2 \in M$ *implies* $x \in M$.

Proof. The necessity of the condition is immediate. If $M = S$ the sufficiency of the condition is trivial, so we assume $M \subset S$. Let $x \in C(M)$, and let the sets Y and Z be defined as in Lemma 6.1. For any $s \in S$, $y \in Y$, $x(ys) = (xy)s \in M$, whence $ys \in Y$; and by Lemma 6.1, $(sy)x = s(yx) \in M$, whence $sy \in Z = Y$. Therefore $YS \subseteq Y$ and $SY \subseteq Y$, whence Y is a two-sided ideal of S. Now $x \notin Y$; for $x \in Y$ implies $x^2 = xx \in M$, whence $x \in M$. Therefore $Y \subset S$, and since $M \subseteq Y$ and M is maximal we have $M = Y$. Hence $xy \in M$ implies $y \in M$, whence M is prime.

From Theorems 6.3 and 6.5 we have at once the

Corollary. *If M is a maximal two-sided ideal in a semigroup S, and if the complement $C(M)$ of M is commutative, then $C(M) \subseteq S^2$ if and only if $x^2 \in M$ implies $x \in M$.*

We present in conclusion the example, to which we have alluded earlier, of a (necessarily infinite and non-commutative) semigroup with two-sided identity element in which the maximal proper two-sided ideal is not prime.

Let N be the set of all non-negative integers, and let S be the semigroup of all single-valued mappings of N into itself, of which $\iota : n \to n$ is a two-sided identity element. Let Σ be the class of all $\varphi \in S$ such that $\varphi(N)$ is a finite subset of N; Σ is clearly a proper two-sided ideal of S, and we proceed to prove that it is maximal by proving that every element in its complement is an internal divisor of ι .

Now $C(\Sigma)$ consists of the mappings φ of N into itself such that $\varphi(N)$ is infinite. Since N is countably infinite, every infinite subset of N is countably infinite. Hence, given any two infinite subsets N_1, and N_2 of N, there exists at least one element $\sigma \in C(\Sigma)$ such that $\sigma(N_1) = N_2$ and σ is a one-to-one correspondence between N_1 and N_2 . Let $\varphi \in C(\Sigma)$, and let $\varphi(N) = M$. For each $m \in M$ let A_m be the complete inverse image $\varphi^{-1}(m)$ of m under φ . Since φ is single-valued, the sets A_m are disjoint; and since φ is everywhere defined on N , the sets A_m exhaust N . Now, calling upon the Axiom of Choice, we may choose from each A_m exactly one element m' ; let M' be the set of elements so chosen. Then the correspondence $m \leftrightarrow m'$ is a one-to-one correspondence between M and M' . But, since M is countably infinite, there is a one-to-one correspondence between N and M . Hence there is a one-to-one correspondence between N and M' . Let ψ be any such correspondence; regarded as a mapping of N into itself, $\psi \in C(\Sigma)$. Now $\varphi\psi(N) = \varphi[\psi(N)] = \varphi(M') = M$, and $\varphi\psi$ is a one-to-one mapping of N into itself. Let χ be any element of $C(\Sigma)$ such that if $n \in N$ and $\varphi\psi(n) = m$ then $\chi(m) = n$. Then, for any $n \in N$, if $\psi(n) = m'$ and $\varphi(m') = m$ and $\chi(m) = n$ then $\chi\varphi\psi(n) = n$, whence $\chi\varphi\psi = \iota$. Hence φ is an internal divisor of ι , whence no proper two-sided ideal of S can contain φ . Therefore Σ is an unique maximal ideal of S .

Finally, we show that Σ is not a prime ideal by exhibiting a pair of elements of $C(\Sigma)$ whose product lies in Σ . Let φ be defined by $\varphi(n) = n + 1$ for n even and $\varphi(n) = n$ for n odd; then $\varphi(N)$ is the set of all odd positive integers. Let ψ be defined by $\psi(n) = n$ for n even and $\psi(n) = 0$ for n odd; then $\psi(N)$ is the set of all even non-negative integers. Thus $\varphi, \psi \in C(\Sigma)$. But, for any $n \in N$, $\psi\varphi(n) = 0$; hence $\psi\varphi \in \Sigma$. Therefore Σ is not a prime ideal of S .

BIBLIOGRAPHY

BIBLIOGRAPHY

Birkhoff, Garrett and MacLane, Saunders. A Survey of Modern Algebra. New York: Macmillan, 1941.

Carman, Kenneth Scott. "Semigroup Ideals." Master's thesis, Knoxville, University of Tennessee, 1949.

Clifford, A. H. and Miller, D. D. "Semigroups Having Zeroid Elements," The American Journal of Mathematics, 70:117-25, 1948.

Dubreil, Paul. Algèbre, v. I. Paris: Gauthier-Villars, 1946.

Harden, John Charles. "Direct and Semidirect Products of Semigroups." Master's thesis, Knoxville, University of Tennessee, 1949.

Huntington, E. V. "Simplified Definition of a Group." Bulletin of the American Mathematical Society, 8:296-300, 1901-2.

McCoy, Neal H. Rings and Ideals. Buffalo: The Mathematical Association of America, 1948.

Posey, Eldon Eugene. "Endomorphisms and Translations of Semigroups." Master's thesis, Knoxville, University of Tennessee, 1949.

Rees, D. "On Semi-groups." Proceedings of the Cambridge Philosophical Society, 36:387-400, 1940.

Rutledge, William A. "Normality in Semigroups." Master's thesis, Knoxville, University of Tennessee, 1948.

Vandiver, H. S. "The Elements of a Theory of Abstract Discrete Semi-groups." Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, 85:71-86, 1940.

Zassenhaus, Hans. Lehrbuch der Gruppentheorie, v. I. Leipzig u. Berlin: Teubner, 1937. [English translation, The Theory of Groups. New York: Chelsea, 1949.]

APPENDIX

APPENDIX

In this appendix, compiled jointly by Messrs. K. S. Carman, J. C. Harden, and E. E. Posey, are listed what the authors believe to be all distinct semigroups of orders two, three, and four, and their proper sub-semigroups. Two semigroups are regarded as distinct if no isomorphism (or anti-isomorphism) can be set up between them.

Commutative semigroups of these orders (under the name of "finite ova") were listed by A. R. Poole in his dissertation,[1] but were omitted from the published version.[2] We have constructed independently all semigroups of orders two and three (non-commutative as well as commutative), and our list of commutative semigroups of those orders agrees perfectly with Poole's.

In addition to constructing the non-commutative semigroups of order four, we have examined Poole's list of commutative semigroups of that order, and have found what appear to be a few errors. It should be pointed out that the copy of Poole's thesis available to us was a carbon copy borrowed from the library of the California Institute of Technology, with the subscripts in the semigroup multiplication tables filled in by hand, so that it is entirely possible that the errors noted do not occur in the original dissertation; indeed, some of these errors are obviously merely mistakes in copying. We did not construct the commutative

---

[1]A. R. Poole, "Finite Ova," (Doctoral Dissertation, California Institute of Technology, 1935).

[2]A. R. Poole, "Finite Ova," The American Journal of Mathematics, 59:23-32, 1937.

semigroups of order four independently, and cannot claim that our examination of Poole's list was sufficiently exhaustive to preclude the possibility that it contains errors other than those noted below.

Poole's R 4_{21} appears as:

u_1	u_1	u_1	u_1
u_1	u_2	u_3	u_2
u_1	u_3	u_1	u_3
u_1	u_2	u_1	u_2

which is non-commutative since $u_4u_3 \neq u_3u_4$. An examination of associativity shows that if $u_4u_3 = u_1$ then the system is not a semigroup regardless of what the product u_3u_4 may be. Changing u_4u_3 from u_1 to u_3, we have a commutative semigroup, distinct from all others in Poole's list, which is given in our list as No. 4.38.

The multiplication table of Poole's R 4_{30} is identical with that of his R 4_{17}; this semigroup appears in our list as No. 4.9. Changing a single subscript yields a new commutative semigroup, No. 4.5 in our list:

R 4_{17}, R 4_{30}					4.5			
u_1	u_1	u_1	u_1		u_1	u_1	u_1	u_1
u_1	u_2	u_1	u_2		u_1	u_2	u_1	u_2
u_1	u_1	u_1	u_1		u_1	u_1	u_1	u_1
u_1	u_2	u_1	u_2		u_1	u_2	u_1	u_4

Poole's T 4_2 and T 4_3 are identical, and appear in our list as No. 4.22. Two changes produce a new commutative semigroup, our No. 4.23:

T 4_2, T4_3

u_1	u_1	u_1	u_4
u_1	u_2	u_1	u_4
u_1	u_1	u_1	u_4
u_4	u_4	u_4	u_1

4.23

u_1	u_1	u_1	u_4
u_1	u_2	u_1	u_4
u_1	u_1	u_3	u_4
u_4	u_4	u_4	u_4

Multiplication table R 4_{15} in Poole's list fails to satisfy the associativity condition, but can be so modified as to become a commutative semigroup apparently distinct from all others in that list; we include it as No. 4.3:

R 4_{15}

u_1	u_1	u_1	u_1
u_1	u_2	u_1	u_1
u_1	u_1	u_1	u_2
u_1	u_1	u_2	u_1

4.3

u_1	u_1	u_1	u_1
u_1	u_1	u_1	u_1
u_1	u_1	u_2	u_2
u_1	u_1	u_2	u_2

Poole's semigroups R 4_2 and R 4_8 seem to be isomorphic; this semigroup appears in our list as No. 4.43. Poole's tables and an isomorphism between them are exhibited below:

R 4_2

u_1	u_1	u_1	u_1
u_1	u_2	u_1	u_1
u_1	u_1	u_3	u_3
u_1	u_1	u_3	u_4

$u_1 \longleftrightarrow u_1$

$u_2 \longleftrightarrow u_4$

$u_3 \longleftrightarrow u_2$

$u_4 \longleftrightarrow u_3$

R 4_8

u_1	u_1	u_1	u_1
u_1	u_2	u_2	u_1
u_1	u_2	u_3	u_1
u_1	u_1	u_1	u_4

In Table Ia are listed the four semigroups of order two, of which only No. 2.3 is non-commutative. Table IIa contains the six non-commutative semigroups of order three (Nos. 3.7, 3.9, 3.12, 3.13, 3.14, 3.15) and the twelve commutative semigroups of order three, the latter being identical (to within isomorphism) with Poole's ova of order three. In Table IIIa we list the 55 commutative semigroups of order four (Nos. 4.1–4.55) and the 66 non-commutative semigroups of order four (Nos. 4.56 – 4.121).

In Table IVa, the columns are headed by the reference numbers of the semigroups of order two, and the rows are labeled with the reference numbers of the semigroups of order three. If No. 3.z (z = 1, ..., 18) contains k subsemigroups isomorphic to No. 2.y (y = 1, ..., 4), the letter k is placed at the intersection of the row 3.z and the column 2.y. Table Va exhibits similarly the subsemigroups of orders two and three of the semigroups of order four. Subsemigroups of order one are simply the idempotent elements of a semigroup, and are not listed separately since they are visible immediately upon inspection of the multiplication table of the semigroup.

It would be futile to expect tables of this sort to be entirely free from errors. The authors have checked their work repeatedly, and have rectified several mistakes, but others have doubtless escaped their notice. They will appreciate receiving corrections from users of the tables.

TABLE Ia

SEMIGROUPS OF ORDER TWO

2.1	2.2	2.3	2.4
1 2	1 1	1 1	1 1
2 1	1 2	2 2	1 1

TABLE IIa

SEMIGROUPS OF ORDER THREE

3.1	3.2	3.3	3.4	3.5	3.6
1 2 2	1 1 1	1 2 3	1 1 3	1 1 3	1 1 1
2 1 1	1 1 1	2 3 1	1 1 3	1 2 3	1 1 1
2 1 1	1 1 2	3 1 2	3 3 1	3 3 1	1 1 3
3.7	**3.8**	**3.9**	**3.10**	**3.11**	**3.12**
1 1 1	1 1 1	1 1 1	1 1 3	1 2 3	1 1 1
1 2 1	1 1 2	2 2 2	1 1 3	2 1 3	2 2 2
1 3 1	1 2 3	1 1 1	3 3 3	3 3 3	1 1 3
3.13	**3.14**	**3.15**	**3.16**	**3.17**	**3.18**
1 1 1	1 1 1	1 1 3	1 1 1	1 1 1	1 1 1
2 2 2	2 2 2	2 2 3	1 2 2	1 2 1	1 1 1
1 2 3	3 3 3	3 3 3	1 2 3	1 1 3	1 1 1

TABLE IIIa

SEMIGROUPS OF ORDER FOUR

4.1	4.2	4.3	4.4	4.5	4.6	4.7
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1
1 2 2 2	1 2 1 1	1 1 1 1	1 2 1 4	1 2 1 2	1 2 1 1	1 1 1 1
1 2 3 3	1 1 1 1	1 1 2 2	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 2
1 2 3 3	1 1 1 1	1 1 2 2	1 4 1 1	1 2 1 4	1 1 1 3	1 1 2 2
4.8	**4.9**	**4.10**	**4.11**	**4.12**	**4.13**	**4.14**
1 1 1 1	1 1 1 1	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 1	1 2 1 1
1 1 1 3	1 2 1 2	2 1 4 3	2 1 4 3	2 3 1 4	2 3 1 2	2 1 2 2
1 1 1 1	1 1 1 1	3 4 2 1	3 4 1 2	3 1 2 4	3 1 2 3	1 2 3 4
1 3 1 2	1 2 1 2	4 3 1 2	4 3 2 1	4 4 4 4	1 2 3 4	1 2 4 3
4.15	**4.16**	**4.17**	**4.18**	**4.19**	**4.20**	**4.21**
1 2 1 2	1 2 1 1	1 2 1 1	1 2 3 1	1 2 3 3	1 2 3 4	1 1 1 4
2 1 2 1	2 1 2 2	2 1 2 2	2 1 3 2	2 1 3 3	2 1 3 4	1 2 3 4
1 2 3 4	1 2 3 1	1 2 3 4	3 3 3 3	3 3 3 3	3 3 3 4	1 3 1 4
2 1 4 3	1 2 1 4	1 2 4 4	1 2 3 4	3 3 3 4	4 4 4 4	4 4 4 1
4.22	**4.23**	**4.24**	**4.25**	**4.26**	**4.27**	**4.28**
1 1 1 4	1 1 1 4	1 1 3 3	1 2 1 4	1 2 4 4	1 1 1 1	1 1 1 1
1 2 1 4	1 2 1 4	1 2 3 4	2 2 2 2	2 2 2 2	1 2 1 4	1 2 3 4
1 1 1 4	1 1 3 4	3 3 1 1	1 2 1 4	4 2 1 1	1 1 1 1	1 3 1 3
4 4 4 1	4 4 4 4	3 4 1 1	4 2 4 1	4 2 1 1	1 4 1 2	1 4 3 2
4.29	**4.30**	**4.31**	**4.32**	**4.33**	**4.34**	**4.35**
1 1 3 1	1 2 1 1	1 2 1 2	1 2 2 2	1 1 3 1	1 1 3 3	1 2 3 3
1 2 3 2	2 1 2 2	2 1 2 1	2 1 1 1	1 1 3 1	1 1 3 3	2 3 1 1
3 3 1 3	1 2 1 1	1 2 1 2	2 1 1 1	3 3 1 3	3 3 1 1	3 1 2 2
1 2 3 2	1 2 1 1	2 1 2 1	2 1 1 1	1 1 3 2	3 3 1 2	3 1 2 2
4.36	**4.37**	**4.38**	**4.39**	**4.40**	**4.41**	**4.42**
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1
1 2 3 3	1 2 3 4	1 2 3 2	1 2 3 4	1 2 2 2	1 2 2 2	1 2 2 2
1 3 1 1	1 3 1 1	1 3 1 3	1 3 1 1	1 2 2 2	1 2 2 2	1 2 3 3
1 3 1 1	1 4 1 1	1 2 3 2	1 4 1 3	1 2 2 2	1 2 2 3	1 2 3 4

TABLE IIIa

SEMIGROUPS OF ORDER FOUR (Continued)

4.43	4.44	4.45	4.46	4.47	4.48	4.49
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1
1 2 2 1	1 2 2 1	1 2 2 4	1 2 2 2	1 2 2 2	1 2 1 1	1 2 1 2
1 2 3 1	1 2 3 4	1 2 3 4	1 2 3 2	1 2 3 4	1 1 3 1	1 1 3 3
1 1 1 4	1 1 4 1	1 4 4 1	1 2 2 2	1 2 4 2	1 1 1 4	1 2 3 4
4.50	4.51	4.52	4.53	4.54	4.55	4.56
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 4
1 2 1 1	1 2 1 1	1 2 1 2	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 4
1 1 3 1	1 1 3 4	1 1 3 1	1 1 1 2	1 1 1 1	1 1 1 1	1 1 2 4
1 1 1 1	1 1 4 1	1 2 1 2	1 1 2 1	1 1 1 2	1 1 1 1	1 1 1 4
4.57	4.58	4.59	4.60	4.61	4.62	4.63
1 1 1 4	1 1 3 4	1 1 1 1	1 2 3 4	1 1 3 4	1 1 1 1	1 1 1 1
1 2 3 4	1 1 3 4	2 2 2 2	2 1 3 4	1 1 3 4	2 2 2 2	2 2 2 2
1 3 2 4	3 3 3 4	1 1 1 2	3 3 3 4	3 3 3 4	3 3 3 3	1 2 3 4
1 1 1 4	3 3 3 4	4 4 4 4	4 4 3 4	4 4 3 4	1 2 2 4	2 1 4 3
4.64	4.65	4.66	4.67	4.68	4.69	4.70
1 1 3 3	1 2 3 4	1 1 1 1	1 1 3 3	1 1 3 3	1 1 1 1	1 1 1 1
2 2 4 4	2 1 4 3	2 2 2 2	2 2 3 3	2 2 3 3	1 1 2 2	2 2 2 2
1 1 3 3	1 2 3 4	1 1 3 3	3 3 3 3	3 3 3 3	1 2 3 4	3 3 3 3
2 2 4 4	2 1 4 3	2 2 4 4	4 4 4 4	4 4 3 3	1 2 3 4	3 3 3 4
4.71	4.72	4.73	4.74	4.75	4.76	4.77
1 1 1 1	1 1 3 4	1 1 3 3	1 1 3 4	1 1 3 3	1 1 1 1	1 1 1 1
2 2 2 2	2 2 3 4	2 2 3 3	2 2 3 4	2 2 3 3	1 1 1 3	2 2 2 2
1 1 1 1	3 3 3 4	3 3 3 3	3 3 3 3	3 3 3 3	1 1 1 3	1 1 1 1
4 4 4 4	3 3 3 4	3 3 3 4	3 3 3 3	3 3 3 3	1 2 3 4	1 1 1 1
4.78	4.79	4.80	4.81	4.82	4.83	4.84
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 4
2 2 2 2	2 2 2 2	2 2 2 2	2 2 2 2	2 2 2 2	2 2 2 2	1 2 1 4
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 3	1 2 3 1	1 1 1 3	1 3 1 4
2 2 2 2	1 1 1 4	2 2 2 4	2 2 2 4	1 1 1 1	1 2 1 4	1 1 1 4

TABLE IIIa

SEMIGROUPS OF ORDER FOUR (Continued)

4.85	4.86	4.87	4.88	4.89	4.90	4.91
1 1 1 1	1 1 1 4	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 4	1 1 1 1
2 2 2 2	2 2 2 4	2 2 2 2	2 2 2 2	2 2 2 2	2 2 2 4	2 2 2 2
1 1 1 3	1 1 1 4	1 1 1 1	1 1 1 3	1 1 1 3	1 1 3 4	1 1 3 1
1 1 3 4	4 4 4 4	1 2 3 4	1 2 3 4	1 1 1 4	4 4 4 4	1 1 1 4
4.92	4.93	4.94	4.95	4.96	4.97	4.98
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 3 4
2 2 2 2	2 2 2 2	2 2 2 2	2 2 2 2	2 2 2 2	2 2 2 2	2 2 3 4
1 1 3 1	1 2 3 1	1 1 3 3	1 1 3 3	3 3 3 3	1 2 3 3	3 3 3 4
2 2 2 4	1 1 1 4	1 1 3 4	1 2 3 4	1 2 3 4	1 2 3 4	4 4 3 4
4.99	4.100	4.101	4.102	4.103	4.104	4.105
1 1 1 4	1 1 3 4	1 1 1 1	1 1 1 4	1 1 3 4	1 1 3 4	1 1 3 4
2 2 2 4	2 2 3 4	2 2 2 2	2 2 2 4	2 2 3 4	2 2 3 4	1 1 3 4
1 2 3 4	3 3 3 3	3 3 3 3	3 3 3 4	3 3 3 4	3 3 3 4	3 3 3 3
4 4 4 4	4 4 4 4	4 4 4 4	4 4 4 4	4 4 4 3	4 4 4 4	3 3 3 3
4.106	4.107	4.108	4.109	4.110	4.111	4.112
1 2 3 4	1 1 1 4	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1
2 1 3 4	1 2 1 4	1 2 1 1	1 2 1 1	1 1 1 1	1 2 1 4	1 1 1 2
3 3 3 3	1 3 1 4	1 3 1 1	1 3 1 1	1 1 1 1	1 3 1 1	1 1 1 1
3 3 3 3	4 4 4 1	1 3 1 1	1 1 1 1	1 2 3 4	1 1 1 1	1 2 3 4
4.113	4.114	4.115	4.116	4.117	4.118	4.119
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 4	1 1 1 1	1 1 1 1	1 1 1 1
1 2 1 1	1 2 1 1	1 2 1 2	1 2 1 4	1 2 1 1	1 2 1 2	1 1 1 2
1 3 1 1	1 3 1 1	1 3 1 3	1 3 1 4	1 3 1 1	1 3 1 3	1 1 3 3
1 3 3 4	1 1 3 4	1 2 1 4	4 4 4 4	1 1 1 4	1 2 3 4	1 1 3 4
4.120	4.121					
1 2 2 1	1 1 1 1					
2 1 1 2	1 1 1 1					
2 1 1 2	1 1 1 2					
1 2 3 4	1 1 1 1					

TABLE IVa

PROPER SUBSEMIGROUPS OF SEMIGROUPS OF ORDER THREE

	2.1	2.2	2.3	2.4
3.1	1			
3.2				1
3.3				
3.4	1			1
3.5	1	1		
3.6		1		1
3.7		1		1
3.8		1		1
3.9			1	1
3.10		1		1
3.11	1	1		
3.12		1	1	
3.13		2	1	
3.14			3	
3.15		2	1	
3.16		3		
3.17		2		
3.18				2

TABLE Va

PROPER SUBSEMIGROUPS OF SEMIGROUPS OF ORDER FOUR

	2.				3.																	
4.	1	2	3	4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1		3		1										2						1		
2		1		2						2												1
3				1		2																
4		1		2						1		1										1
5		3		1						2										1		
6		1		1		1				1												
7				2		1																1
8				2																		1
9		1		2						1				1								
10	1																					
11	2																					
12		1					1															
13		1					1															
14	2								1						1							
15	2								1													
16	1	2							2												1	
17	1	3							2											1		
18	1	3							1						1					1		
19	1	3													1						1	
20	1	3													2					1		
21	1	1		1				1	1			1										
22	1	1		1				1	1	1												
23		5																		2	1	
24	1	1			1				1													
25	1	1		1				1						1	1							
26	1	1			1										1							
27		1		1						1					1							
28		1		1								1			1							
29	1	1							1					1								
30	1			2				2														1
31	1			1	1			1														
32	1				2																	
33	1			1		1		1														
34	1			1				1														
35							1															
36		1		2								1										1
37		1		2								1										1
38		1		2								1		1								
39		1		1		1						1										
40		1		2										2								1
41		1		1		1								1								

TABLE Va

PROPER SUBSEMIGROUPS OF SEMIGROUPS OF ORDER FOUR
(Continued)

	2.				3.																	
4.	1	2	3	4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
42		6																		4		
43		4																		1	2	
44		3								1		1								1		
45		3										2								1		
46		3								1				1						1		
47		3		1								1		1						1		
48		3																			3	
49		4																		2	1	
50		2		1						2											1	
51		2		1						1		1									1	
52		2												1							1	
53				3																		2
54				2		1																1
55				3																		3
56			1	1		1							1									
57	1	1	1												1	1						
58		1	1	1										1		1						
59			3	1									1					1				
60	1	1	1												2		1					
61		2	1	1										2			1					
62		2	3													1	1	1				
63	1	2	1														1					
64			3																			
65	2		1																			
66		1	2													2						
67		2	2													2			1			
68		2	1	1							2								1			
69		2	1	1								2							1			
70		1	3													2		1				
71			3	1									2					1				
72		1	2													2			1			
73		3	1																1		2	
74		2	1	1							2								1			
75		2	1	1						2									1			
76		1		2								1										1
77			1	2									2									1
78			1	2									2									
79		1	1	1						1			1			1						
80		1	1	1									1			1						
81		1	1	1									1			1						
82		2	1	1		1							1				1					

TABLE Va

PROPER SUBSEMIGROUPS OF SEMIGROUPS OF ORDER FOUR
(Continued)

	2.				3.																	
4.	1	2	3	4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
83		2	1	1							1		1				1					
84		1	1								1		1			1						
85		1	1	1								1	1			1						
86		2	1	1									1	1					1			
87		2	1	1							1		1				1					
88		2	1	1								1	1				1					
89		1	1	1							1		1			1						
90		4	1													1			1	1		
91		2	1													2					1	
92		2	1													2						
93		3	1													1	1			1		
94		3	1													2				1		
95		4	1													1	1			1		
96		3	3														3	1				
97		5	1														2			2		
98		4	2														2		2			
99		5	1														1		1	2		
100		4	2															2	2			
101			6															4				
102		3	3															1	3			
103	1	2	1						2										1			
104		5	1																2	2		
105		1		2							1			1								
106	1	1		1							1				1							
107	1	1		1				1	1		1											
108		1		2							1											1
109		2		1						1	1										1	
110		1		2							2											1
111		1		2							2											1
112		1		2							1	1										1
113		2		1							2											
114		2		1							2										1	
115		3		1							1									2		
116		3		1							1			1						1		
117		2		1						1	1										1	
118		3		1							1	1								1		
119		3		1						1	1									1		
120	1	1			1				1													
121			3																			2