A semigroup is a set of elements to which is related an operation usually called multiplication and an equivalence relation, such that the set is closed and associative relative to the operation.

We shall discuss, briefly, finite semigroups which are uniquely factorable in the same sense as the multiplicative semigroup of all nonzero integers. Clifford\(^1\) defined an arithmetic in such a way as to include our uniquely factorable semigroups as well as similar infinite commutative semigroups, not necessarily cancellable, and gave necessary and sufficient conditions for a commutative semigroup to be imbedded in an arithmetic. He used ideals to accomplish this imbedding. We shall accomplish a constructive imbedding of any finite commutative semigroup of idempotents alone in a uniquely factorable semigroup, by the use of correspondences, or generalized substitutions. This method of imbedding is the chief novelty herein.

Let a finite commutative semigroup \(S\) contain an identity, and \(U\) be the set of units, or divisors of the identity. Then \(U\) is a group, and \(S\) can be divided exhaustively into disjoint cosets\(^2\) relative to \(U\). This division into cosets is unique, and the cosets form a semigroup, designated by \(S/U\), whose identity is \(U\), such that \(S/U\) is a homomorphic image of \(S\). We shall use \(=\) and \(\approx\) as the equivalence relations of \(S/U\) and \(S\), respectively. If \(s \in S\), the elements of the coset \(sU\) are called associated elements or associates.

If \(S\) is a finite semigroup, \(a \in S\), and \(k\) and \(s\) are the least positive integers such that \(k < s\) and \(a^s = a^k\), then \(s - 1, k\), and \(s - k\) are called, respectively, the order, index, and period of \(a\).

The semigroup \(S\) is called a uniquely factorable semigroup, abbreviated “UFS,” provided that \(S\) is finite and commutative and contains at least two elements, one of which is a unit, and satisfies:

(i) There exists an element in \(S/U\), called a prime, and denoted by \(P\), such that the only divisors of \(P\) are \(U\) and \(P\).

(ii) Each element of \(S/U\) has unity for its period.

(iii) Each element of \(S/U\) is expressible uniquely, except for order, as a product of powers of distinct primes.

Note that if \(P_i\) and \(P_j\) are the highest powers of the prime \(P\) which appear, respectively, in two factorizations of an element of \(S/U\), it follows that \(P_i = P_j\) but not necessarily that \(i = j\).

Properties of Uniquely Factorable Semigroups.—The first five of the properties below follow from the fact that \(S/U\) is a homomorphic image of \(S\).

1. If \(S\) is a UFS, so also is \(S/U\).

2. If \(S\) is a UFS and \(p \in S\), then \(p\) is prime in \(S\) (has no other divisors than units and its associates) if and only if the coset \(pU\) is prime in \(S/U\).
3. Let $S$ be a UFS, $i$ be an idempotent of $S$, and $G$ be the maximal subgroup of $S$ with $i$ as its identity; then $G = iU$.

4. If $S$ is a UFS, $s \in S$, $s \in U$, $s$ has index $j$, and $sU$ has index $k$, then $j = k$.

5. If $S$ is a UFS, $s \in S$, $s \in U$, and two complete factor decompositions of $s$ in $S$ are described by $s = u_1 \left( \prod_{n=1}^{a} (p_n)^{i_n} \right) = u_2 \left( \prod_{n=1}^{b} (q_n)^{j_n} \right)$, with the $i$'s and $j$'s equal to or less than the indices of the $p$'s and the $q$'s, respectively, and $u_1, u_2 \in U$, then the $q$'s are associates of the $p$'s in some order, $a = b$, and the corresponding exponents are equal.

6. If $S$ is a UFS, $P_1, P_2, \ldots, P_n$ are the nonequivalent primes of $S/U$, and if these primes generate, respectively, the cyclic groups $S_1, S_2, \ldots, S_n$, and + denotes set union, then $S/U$ is isomorphic to the direct product $(S_1 + U) \times (S_2 + U) \times \ldots \times (S_n + U)$.

Proof: Let the orders of $P_1, P_2, \ldots, P_n$ be $o_1, o_2, \ldots, o_n$, and consider the distinct elements, for $i = 1, 2, \ldots, n$ of the sets $U, \pi_1, \pi_2, \ldots, \pi_n$, where $\pi_i$ is the set $P_i, P_i^2, \ldots, P_i^{o_i}$, and $\pi_j, j = 2, 3, \ldots, n$ denotes the set of all products of all the powers of the distinct primes of $\pi_1$, taken $j$ at a time. No two elements contained in any of the sets above are equal; otherwise condition (iii) would be violated; and the totality of these elements are the distinct elements of the semigroup $S = (S_1 + U)(S_2 + U)\ldots(S_n + U)$, which is isomorphic to the direct product in the statement of the theorem, since $U$ is the intersection of each pair of parenthesized semigroups.

7. If $S$ is a UFS, each of which is an idempotent, then $S$ is expressible as a direct product $(p_1 + e) \times (p_2 + e) \times \ldots \times (p_n + e)$, where the $p$'s are the prime idempotents of $S$ and $e$ is the identity of $S$.

This property is an immediate consequence of property 6.

8. If $S_i$ is a semigroup of order 2 with zero, $0_i$, and identity, $e_i$, for $i = 1, 2, \ldots, n$, then $S = S_1 \times S_2 \times \ldots \times S_n$ is a UFS.

Proof: $S$ is commutative, since each $S_i$ is commutative. Condition (i) is satisfied, since the irreducible elements, or primes, $P_i = (e_1, e_2, \ldots, e_{i-1}, e_i, e_{i+1}, \ldots, e_n)$ generate $S$. Condition (ii) is satisfied, since each idempotent has period 1, and since $S$ is isomorphic to $S/U$. Condition (iii) is satisfied by definition of direct product.

9. If $S$ is a UFS and $C \subseteq S/U$, and $C = \prod_{n=1}^{t} (P_n)^{i_n}$ is a factorization of $C$ into powers of distinct primes, then the index of $C$ is the index of the $(P_n)^{i_n}$ with greatest index.

Proof. By condition (ii) the period of $C$ is 1. Let the index of the $(P_n)^{i_n}$ with greatest index be $j$, and the index of $C$ be $k$. Then by condition (ii),

\[ \prod_{n=1}^{t} (P_n)^{i_nj} = \prod_{n=1}^{t} (P_n)^{i_n} = C^{j+1} = C^j. \]

Hence $j \geq k$. But $C^{k+1} = C^k = \prod_{n=1}^{t} (P_n)^{i_n}$. It follows from condition (iii) that $i_nk$ and $i_nj$ are each greater than or equal to the index of $P_n$; and, by the definition of the index of $(P_n)^{i_n}$, $k \geq j$. But $j \geq k$; therefore, $j = k$.

Correspondences.—$C$ is said to be a correspondence on the set $N$, provided that
Consider theory, a correspondence may have repeated elements in $N$. This is described by $C(a) = b$. We think of a substitution as being a particular correspondence. If we use the double-lined notation of substitution group theory, a correspondence may have repeated elements in the second line. We define equivalence, $\equiv$, of correspondences by $C_1 \equiv C_2$ if and only if $C_1(a) = C_2(a)$ for each $a \in N$, and the product $C_1 C_2$ of correspondences by $C_1 C_2(a) = C_2(C_1(a))$ for each $a \in N$. It follows that each closed set of correspondences is a semigroup. Vandiver and the writer gave examples of the above and other definitions for correspondences and stated a number of results about them.

Let $S$ be a semigroup of correspondences on a set $N$ and $n, e \in N$, such that if $C \in S$, then $C(e) = e$, and, further, $C(n) = e$ implies that $n$ is $e$; then $e$ is called extraneous relative to $S$.

**Lemma 1.** If $S$ is a semigroup of correspondences on $N$ and $e$ is extraneous relative to $S$, then $S$ is isomorphic to a semigroup $S'$ on the set $N'$ obtained by deleting $e$ from $N$.

**Outline of proof:** Equivalence in $S$ is independent of $e$. If for each $C \in S$, and $n \in N'$, we define $C'$ by $C(n) = C'(n)$, then it follows that the $(C')$'s form a semigroup $S'$ which is isomorphic to $S$.

If a semigroup of correspondences $S$ operates on a set $N$ and no element of $N$ is extraneous relative to $S$, then $N$ is called a reduced set for $S$.

**Lemma 2.** For each commutative semigroup $S$ composed only of idempotent correspondences on a set $N$, there exist an isomorphism $H$ and $b \in N$ such that if $C \in S$, $H(C) = C'$, and a $e \in N$ for which $C'(b) = b$, and whenever $C(a) \neq a$, then $C'(a) = b$, but if $C(a) = a$, then $C'(a) = a$.

**Outline of proof:** For each $C \in S$, we define $C'$ such that if $a \in N$ and $C(a) = a$, then $C'(a) = a$, and such that if $d \in N$ and $C(d) \neq d$, then $C'(d) = b$, where $b \in N$ such that for each $C \in S$, $C(b) = b$. The element of $N$ which the zero element of $S$ maps onto itself satisfies this description of $b$. We consider the three cases $C_1(a) = C_2(a) = a$, $C_1(a) = a \neq C_2(a) = d$, and $C_1(a) = d \neq a$, $C_2(a) = e \neq a$, from which case it follows that $C_1 C_2(a) \neq a$. We find in each case that $C_1 C_2'(a) = (C_1 C_2)'(a)$. It follows that the set $S'$ of $(C')$'s is a semigroup and that if $H$ is a mapping such that $H(C) = C'$, then $H$ is an isomorphism.

**Theorem.** Each commutative semigroup $S$ each element of which is an idempotent can be imbedded in a UFS.

**Proof:** If $S$ contains only one idempotent, we adjoin a zero element to obtain the desired UFS. It is known that each finite semigroup can be imbedded in a semigroup of correspondences. The proof is constructive and similar to the usual proof of Cayley's theorem. Hence, by this theorem and Lemmas 1 and 2, each finite commutative semigroup $S$ of idempotents alone can be imbedded in a semigroup $S'$ on a reduced set $N$ for $S'$ such that there exists $m_0 \in N$ for which $C'(m_0) = m_0$, and, if $C' \in S'$, $a \in N$, and $C'(a) \neq a$, then $C'(a) = m_0$. We denote the elements of $N$ by $m_0, m_1, \ldots, n$, and consider the correspondences $E, P_i, P_n, \ldots$, defined by $P_i(m_0) = m_0, P_i(m_j) = m_j$ for $j = 0, 1, \ldots, n$, except $j = i$, and for $i = 1, 2, \ldots, n$, and $E(m_i) = m_i$ for $i = 0, 1, \ldots, n$. Each of these $P$'s is a nonidentity idempotent. Consider the semigroups $S_i, i = 1, 2, \ldots, n$, such that $S_i$ is of order 2 and contains $E$ and $P_i$. Since each $S_i$ satisfies the hypothesis of property 8 for UFS's, it follows that the semigroup $S^* = \Pi_{i=1}^n S_i$, which is isomorphic to the
direct product of the $S_i$'s, is a UFS. $S''$ contains $S'$, since for $C' \in S'$, such that

$$C' \cong \left( \begin{array}{ccc} m_1 m_2 & \ldots & m_r m_0 \\ m_0 m_0 & \ldots & m_0 m_0 \end{array} \right), \ r \leq n,$$

we may select a set $Q_1, Q_2, \ldots, Q_r$ of elements of the set of $P$'s such that for $i = 1, 2, \ldots, r$, $Q_i(m_i) = m_0$, $Q_i(m_0) = m_0$, $\prod_{i=1}^{r} Q_i \cong C'$. Hence $S''$ contains a semigroup which is isomorphic to $S'$, and $S$ is imbedded in $S''$.

**Example:** Imbed the semigroup $S$, whose multiplication table appears below, in a UFS.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>a</td>
<td>0</td>
<td>a</td>
<td>b</td>
<td>0</td>
</tr>
<tr>
<td>b</td>
<td>0</td>
<td>b</td>
<td>b</td>
<td>0</td>
</tr>
<tr>
<td>c</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>c</td>
</tr>
</tbody>
</table>

The semigroups $S'$ and $S''$, described in the proof of the theorem, have elements described by

$$S': \left( \begin{array}{ccc} 0 & a & b & c \\ 0 & 0 & 0 & 0 \end{array} \right), \left( \begin{array}{ccc} 0 & a & b & c \\ 0 & a & b & 0 \end{array} \right), \left( \begin{array}{ccc} 0 & a & b & c \\ 0 & 0 & 0 & 0 \end{array} \right);$$

$$S'': \text{the union of } S' \text{ with the elements}$$

$$\left( \begin{array}{ccc} 0 & a & b & c \\ 0 & 0 & b & c \end{array} \right), \left( \begin{array}{ccc} 0 & a & b & c \\ 0 & a & 0 & c \end{array} \right), \left( \begin{array}{ccc} 0 & a & b & c \\ 0 & a & 0 & 0 \end{array} \right), \left( \begin{array}{ccc} 0 & a & b & c \\ 0 & a & b & c \end{array} \right).$$

The constructive proof mentioned in footnote 4, together with Lemma 2, is useful in constructing $S'$. The three underlined elements above are the $P$'s mentioned in the proof. They are also the primes of $S''$.

* The work on this paper was done in part under National Science Foundation Grant G1397.


