Journal of Gakugei, Tokushima University
Vol. IV, 1954

ON FINITE ONE-IDEMPOTENT SEMIGROUPS (1)

Takayuki TAMURA

Mathematical Institute, Gakugei College, Tokushima University.

(Received September 15, 1953)

Since a finite semigroup contains at least one idempotent [1], [2], the number or the behaviour of idempotents plays an important part in the theory of finite semigroups. As the simplest case, we argue in this paper the structure of a finite one-idempotent semigroup, by which we mean a finite semigroup having only one idempotent. However the precise discussions are here limited to some special cases, and so the others will be called to account in the part II (which is unpublished). In § 1 we relate to the group that is called " Kerngruppe ", and in § 2 give the condition for a one-idempotent semigroup to be a group. Especially we investigate the enclosed extension of a group in § 3, the zero-semigroup in § 4, and the power-semigroup in § 5.

§ 1. Greatest group.

Let S be a finite semigroup whose only one idempotent is e.

Lemma 1. *If a finite one-idempotent semigroup S satisfies $Se=S$ (or $eS=S$), then S is a group.*

Proof. Our proof is only restricted to the case that $Se=S$, the other being analogous. For all $x \in Se$, when x is represented by $x=ye$, $y \in S$, we get $xe=(ye)e=y(ee)=ye=x$. Hence e is a right-identity of Se. Since xS is a subsemigroup of S, it contains this e, in other words, there exists $z \in S$ such that $xz=e$ for any $x \in S$. Thus S has been proved to be a group.

Theorem 1. *Let S be a finite one-idempotent semigroup and let $G=Se$. Then the subset G has the following properties:*

(1) *G is the greatest group*[1] *in S, and $G=eS$.*

(2) *G is the least ideal of S.*

(3) *e commutes with every $x \in S$.*

(4) *S is homomorphic on G.*

---

1) By the greatest group G in S we mean the group G such that $G \supset G_1$ for all group G_1 contained in S. The least ideal is dually defined.

Proof. (1) G is a subsemigroup whose idempotent is no other than e, and satisfies $Ge = G$. It follows from Lemma 1 that G is a group. Since e is the identity of the group G, we have $Se = G = Ge = eG \subset eS$, similarly $eS \subset Se$; and so $Se = eS$. Next, let G_1 be any group contained in S. The element e is at the same time an identity of G_1, and we have $G_1 = G_1 e \subset Se = G$, showing that G is the greatest group in S.

(2) Immediately it follows that

$$SG = S(Se) = (SS)e \subset Se = G\,, \text{ and similarly } GS \subset G\,.$$

Hence G is an ideal. Let Q be any ideal of S. Then $e \in Q$, for Q is a subsemigroup of S. Therefore we have $G = Se \subset SQ \subset Q$. This shows that G is the least ideal of S.

(3) By dint of the fact that e commutes with every element xe of G, we get

$$xe = x(ee) = (xe)e = e(xe) = (ex)e = e(ex) = (ee)x = ex\,.$$

(4) The mapping φ of S onto $G = Se$ is defined as $\varphi(x) = xe$. This φ is proved to be a homomorphism by the formula:

$$\varphi(x)\varphi(y) = (xe)(ye) = x(ey)e = x(ye)e = (xy)(ee) = (xy)e = \varphi(xy)$$

where $x, y \in S$ and $ey = ye$ because of the above (3). q. e. d.

In particular if e is a right (left) identity, S is a group by Lemma 1. If e is a right (left) zero, e is a two-sided zero. Then, however, Theorem 1 becomes trivial, whence we must investigate this case on different standpoints (cf. § 4).

All one-idempotent semigroups of order[2] n are classified into n classes according to the order $k\,(k = 1, 2, \cdots, n)$ of the greatest group in itself. We call the order n the *d-order n of S*, and call the order k the *g-order of S*, or we say that S is of g-order k under d-order n. Especially when S is of g-order 1, S is called a zero-semigroup[3] or z-semigroup.

§ 2. *v*-order and the condition for a group.

The subset SS or S^2 is called the value-range of the semigroup S. When the order of the value-range is m, we say that S is of *v-order m*. This v-order plays a remarkable rôle in our theory as much as the g-order does.

---

2) By "order of S" we mean the number of elements of S.

3) "Zero-semigroup" defined here is more general than what was done by Rees.

Among the above three kinds of orders, n, m, k, obviously holds $k \leqq m \leqq n$. If the v-order of S equals to its d-order, S is said to be universal.

Now, with respect to universal one-idempotent semigroups, the following Theorem 2 is worthy of our notice. In the below Lemma 2, S is not necessarily one-idempotent.

Lemma 2. *Let S be a finite universal semigroup with a zero. If S has a non-void subset X such that $X \subset SX$ and $X \cap S(S-X) = \phi$, then S contains an idempotent different from zero.*

Proof. Let n be the d-order of S and l the order of X. We shall prove the lemma by induction with respect to l. At first when $l=1$, setting $X=\{p\}$, $p \neq 0$[4], we have $p = xp$ for some $x \in S$. Let us denote by A the set of above x for fixed p, then $0 \bar{\in} A$ and A forms a subsemigroup because $(xy)p = x(yp) = xp = p$ for $x, y \in A$; and so A contains an idempotent, consequently S has an idemptotent, which is different from zero.

Next, we shall prove the case for l under the assumption that the lemma holds for $i \leqq l-1$. Take any $a \in X$ such that $Sa \cap X \neq \phi$, then we may assume $Sa \not\supset X$ without losing generality. For, if there is an element a which satisfies $X \subset Sa$, $a \in X$, it follows that $a = xa$ for some $x \in S$; and then we can apply again the method used in the case when $l=1$.

Now, let $X_1 = X - Sa \cap X (\neq \phi)$, we get $S(S-X_1) = S(S-X) \cup Sa$, and $X_1 \cap S(S-X) \subset X \cap S(S-X) = \phi$, while $X_1 \cap Sa = \phi$. Hence $X_1 \cap S(S-X_1) = \phi$. Furthermore, since S is universal, $X_1 \subset SS = S(S-X_1) \cup SX_1$, so that $X_1 \subset SX_1$. X_1 being of order less than l, the supposition of induction enables us to conclude that S has an idempotent which is not zero. This complets the proof.

Corollary. *If S is a finite zero-semigroup, then S is non-universal.*

Proof. Suppose that S is universal. Setting $X = S - \{0\}$, X satisfies the condition of Lemma 2. Therefore S contains an idempotent different from zero, contradicting with the assumption.

Theorem 2. *Let S be a fimte one-idempotent semigroup. If S is universal, then S is a group.*

Proof. Let us suppose that S is not a group. Then, by Theorem 1, S has the greatest group $G(\neq S)$ which is an ideal at the same time, that is, $k < n$[5]

---

4) The condition $X \cap S(S-X) = \phi$ leads to $p \neq 0$.

5) We denote by n the d-order, by k the g-order of S respectively.

according as notations in the end of §1. Denote by S^* the difference semigroup of S modulo G, which is due to Rees [2]. Clearly S^* is a zero-semigroup of order i, $2 \leqq i < n$. Now, let a^* be an arbitrary non-zero element of S^*.

Then the inverse image $a(\in S)$ of a^* is represented as $a = bc$[6], where $b \in S-G$, $c \in S-G$, for S is universal. Hence $a^* = b^*c^*$ where $b^* \in S^*$, $c^* \in S^*$; it follows that S^* is universal. This conflicts with the Corollary.

From Theorem 2, we conclude that if a semigroup S has g-order less than d-order, S is non-universal.

§3. Enclosed extension of a group.

If the value-range S^2 of S coincides with its greatest group G and S is not a group, S is called an enclosed extension of the group G. This paragraph is an attempt to clear its structure. Now let us denote by $a_i (i = 1, \cdots, k)$ all elements of G and by p_i the number of elements $x \in S$ which are mapped into $a_i \in G$ by the homomorphism φ which is introduced in the proof of (4) of Theorem 1. Of course $p_i \geqq 1$. Then an enclosed extension $S = \{a_1, \cdots, a_n\}$ of the group $G = \{a_1, \cdots, a_k\}$, $k < n$, is associated with an ordered system of positive integers $(p_1, \cdots, p_k)$ where $\sum_{i=1}^{k} p_i = n$.

The system $(p_1, \cdots, p_k)$ is termed the character of S, because the system determines S as the following theorems indicate.

Theorem 3. *If there are given a group $G = \{a_1, \cdots, a_k\}$, a set $S = \{a_1, \cdots, a_k, \cdots, a_n\}$ which contains G, and an ordered system of positive integers $(p_1, \cdots, p_k)$ where $\sum_{i=1}^{k} p_i = n$, $p_i \geqq 1$, then an enclosed extension S of G admitting $(p_1, \cdots, p_k)$ to be its character is determined uniquely except for isomorphism.*

Proof. At first we assign a mapping $\varphi : a_i \overset{\varphi}{\rightarrow} \varphi(a_i) = ea_i = a_i e$[7] $(i = 1, \cdots, n)$ such that φ has $(p_1, \cdots, p_k)$ as its character, in other words, the number of elements $x \in S$ which fulfil $\varphi(x) = a_i$ is p_i $(i = 1, \cdots, k)$. We can then prove that the extension S is uniquely constructed under the above φ. In fact, let us define the product xy in S as $xy = \varphi(x)\varphi(y)$[8]. Then, since φ maps an element of G into itself, we have $\varphi(xy) = \varphi(x)\varphi(y)$ which proves that φ is a homomorphism. Conversely it is obvious that the above definition of xy in S is necessary under the assumption that φ is a homomorphism.

Next, we shall prove the uniqueness of S except for isomorphism. Let,

---

6) Of course $b \neq 0$, $c \neq 0$, so that $b^* \neq 0^*$, $c^* \neq 0^*$.

7) e is an idempotent of S, i.e., the unit of G; and of course $\varphi(a_i) \in G$.

8) The product in the right side is that in G.

now, φ' be another mapping (of S on G) which has a character in common with φ; and then it is sufficient to show that two semigroups obtained by φ and φ' are isomorphic each other. Now the common character of φ and φ' enables us to give a permutation[9] ψ of S on itself associating x with one of elements x', which satisfy

(1) $x' = x$ for $x \in G$,

(2) $\varphi'(x') = \varphi(x)$ for $x \in S$.

Then we get, for every $x, y \in S$,

$$\begin{aligned} \psi(x)\psi(y) &= \varphi'(\psi(x)\psi(y)) && (\because\ \psi(x)\psi(y) \in G, \text{ and } \varphi'(z) = z \text{ for } z \in G) \\ &= \varphi'(\psi(x))\varphi'(\psi(y)) && (\text{by homomorphism}) \\ &= \varphi(x)\varphi(y) && (\text{by (2)}) \\ &= \varphi(xy) && (\text{by homomorphism}) \\ &= xy && (\because\ \varphi(z) = z \text{ for } z \in G) \\ &= \psi(xy). && (\text{by (1)}) \end{aligned}$$

Therefore ψ is an isomomorphism. Thus the theorem has been proved.

Now, G and n given, under what condition is an extension obtained by $(p_1, \cdots, p_k)$ isomorphic with that obtained by $(q_1, \cdots, q_k)$? Generally, when $(p_{i_1}, \cdots, p_{i_k})$ is got by permutating $(p_1, \cdots, p_k)$, we denote it by

$$(p_{i_1}, \cdots, p_{i_k}) = \sigma(p_1, \cdots, p_k) \qquad \text{where } \sigma = \begin{pmatrix} 1 & 2 & \cdots & k \\ i_1 & i_2 & \cdots & i_k \end{pmatrix};$$

that is, we say that $(p_1, \cdots, p_k)$ is permutated to $(p_{i_1}, \cdots, p_{i_k})$ by σ. Similarly, if we apply σ to G, we mean a permutation in G written

$$\sigma\{a_1, \cdots, a_k\} = \{a_{i_1}, \cdots, a_{i_k}\} \quad \text{where } a_j \xrightarrow{\sigma} a_{i_j},$$

or we say that $(a_1, \cdots, a_k)$ is permutated to $(a_{i_1}, \cdots, a_{i_k})$.

Theorem 4. *There are given the set $S = \{a_1, \cdots, a_n\}$ and the group $G = \{a_1, \cdots, a_k\}$. Let us denote by S_p an enclosed extension of G with a character $(p_1, \cdots, p_k)$, by S_q one with $(q_1, \cdots, q_k)$, and suppose that a_1 is an idempotent in each of S_p and S_q. In order that S_p is isomorphic with S_q, it is necessary and sufficient that the following conditions are satisfied.*

(1) $p_1 = q_1$.

(2) *There exists a permutation σ such that*

a) *$(p_1, \cdots, p_k)$ is permutated to $(q_1, \cdots, q_k)$ by σ, and*

b) *the mapping $\{a_1, \cdots, a_k\} \to \sigma\{a_1, \cdots, a_k\}$ is an automorphism in the group G.*

9) A permutation is a one to one mapping of S onto itself.

Proof. At first we shall prove the necessity of the theorem. Let us suppose that S_p is mapped isomorphically on S_q by η. Since the greatest group of S_p is mapped on that of S_q by η, the contraction σ of η to G is an automorphism of G. It is obvious that $(p_1, \cdots, p_k)$ is permutated to $(q_1, \cdots, q_k)$ because of the isomorphism η. Now by φ_p and φ_q we mean homomorphisms of S_p and S_q on G respectively. Then we have $p_1 = q_1$, because the idempotent of S_p is mapped to the idempotent of S_q and $\varphi_p(x) = a_1$ implies $\varphi_q(\eta(x)) = a_1$.

Next, we shall prove the sufficiency. Suppose that $(p_1, p_2, \cdots, p_k)$ and $(p_1, q_2, \cdots, q_k)$ satisfy the conditions (1) and (2) in this theorem. Then we can define a permutation η of S_p on S_q i.e., $\{a_{j(1)}, \cdots, a_{j(n)}\} = \eta\{a_1, \cdots, a_n\}$ with the properties as follow:

(1) the contraction η to G coincides with σ,

(2) $j(i) = i$ for $i=1, k+1, k+2, \cdots, n$.

(3) $\eta(ex) = e \cdot x$ where $e \cdot x$ is the product in S_q.

Considering that $xy = (ex)(ey)$ for $x, y \in S_p$, $x \cdot y = (e \cdot x) \cdot (e \cdot y)$ for $x, y \in S_q$, and $\eta(x) = x$ for $x \in S-G$, we have

$$\eta(xy) = \eta((ex)(ey)) = \eta(ex)\eta(ey) = (e \cdot x) \cdot (e \cdot y) = x \cdot y = \eta(x) \cdot \eta(y) \text{ for } x, y \in S-G,$$
$$\eta(bx) = \eta(b(ex)) = \eta(b) \cdot \eta(ex) = \eta(b) \cdot (e \cdot x) = \eta(b) \cdot x \text{ for } b \in G,\ x \in S-G.$$

Similarly $\eta(xb) = x \cdot \eta(b)$ for $b \in G$, $x \in S-G$.

Hence η proves to be an isomorphism of S_p on S_q. Thus the proof of the theorem has been completed.

§ 4. Zero-semigroups.

In this paragraph we shall relate to some remarkable properties of a zero-semigroup S. Let us denote by 0 the zero of S. We mean by an annihilator of S an element $a \in S$ which satisfies $ax = xa = 0$ for all $x \in S$. Of course a two-sided zero is an annihilator. The following theorem is of significance for the study of its structure.

Theorem 5. *A finite zero-semigroup S of d-order no less than 2 has at least one annihilator except the zero.*

Proof. The theorem holds if the d-order is 2, since a zero-semigroup of d-order 2 is no other than

	0	a
0	0	0
a	0	0

.

We shall prove the theorem for n under the assumption of validity for $n-1$. By the corollary in § 2, S has a subset[10] S_{n-1} such that $S^2 \subset S_{n-1}$, for which we set $S = S_{n-1} \cup \{p\}$, $p \bar{\in} S_{n-1}$. Since S_{n-1} is clearly a zero-semigroup, we can find a non-zero annihilator b of S_{n-1}. Here we may assume that either $bp \neq 0$ or $pb \neq 0$. For if $bp = pb = 0$, b becomes an annihilator of S, solving the present problem. Now, let us consider the element $c = pbp$ in S, for which the two cases may be considered: $c = 0$, $c \neq 0$.

(1) When $c = 0$ with $bp \neq 0$, it will be proved that bp is an annihilator of S.

In fact, clearly $p(bp) = 0$ and $z(bp) = (zb)p = 0p = 0$ for $z \in S_{n-1}$,
while $(bp)z = b(pz) = 0$ for $z \in S_{n-1}$ because $pz \in S_{n-1}$.

It follows that $bp (\neq 0)$ is an annihilator of S.

(2) When $c \neq 0$, c itself is one required.
Because, for every $z \in S$,

$$(pbp)z = p\{b(pz)\} = p0 = 0, \text{ and } z(pbp) = \{(zp)b\}p = 0p = 0$$

Since pz, $zp \in S_{n-1}$. Thus we completes the proof.

Theorem 6. *Let S be a zero-semigroup of d-order n. We can put all elements of S in order*

$$a_1, a_2, \cdots, a_n,$$

such that, setting $S_i = \{a_1, \cdots, a_i\}$, it holds that

$$SS_i \subset S_{i-1} \text{ and } S_iS \subset S_{i-1} \text{ for } i = 2, 3, \cdots, n.$$

Proof. Let a_1 be the zero and a_2 be an annihilator different from zero. (see Theorem 5.) Obviously $S_2S \subset S_1 \subset S_2$, $SS_2 \subset S_1 \subset S_2$; S_2 is an ideal of S. Now, after the ideal $S_{i-1} = \{a_1, \cdots, a_{i-1}\}$ (for $i \geqq 3$) is constructed such that $S_{i-1}S \subset S_{i-2}$ and $SS_{i-1} \subset S_{i-2}$, we obtain S_i by adding a_i whose image $a_i^{(i-1)}$ into the difference semigroup[11] $S^{(i-1)} = (S : S_{i-1})$ of S modulo S_{i-1} is a non-zero annihilator, that is, $a_i^{(i-1)} S^{(i-1)} \subset \{0^{(i-1)}\}$ and $S^{(i-1)} a_i^{(i-1)} \subset \{0^{(i-1)}\}$. Consequently we have $a_iS \subset S_{i-1}$, $Sa_i \subset S_{i-1}$. Then it follows immediately

$$S_iS = S_{i-1}S \cup a_iS \subset S_{i-2} \cup S_{i-1} = S_{i-1},$$

similarly $SS_i \subset S_{i-1}$. The proof of the theorem has been accomplished.

---

10) S_{n-1} is composed of $n-1$ elements.

11) Rees denoted by $S^* = S - G$ the difference semigroup S^* of S modulo G, but we denote it by $S^* = (S : G)$.

By Theorem 6, one part of the structure of one-idempotent semigroups is clarified.

Theorem 6′. *Let S be a one-idempotent semigroup of d-order n. We can put all elements of S in order*

$$a_1, a_2, \cdots, a_k, a_{k+1}, \cdots, a_n$$

such that

(1) *$G=\{a_1, \cdots, a_k\}$ is the greatest group of S.*

(2) *Setting $S_i=\{a_1, \cdots, a_i\}$, it holds that*

$$SS_i \subset S_{i-1} \text{ and } S_iS \subset S_{i-1} \text{ for } i=k+1, k+2, \cdots, n.$$

§ 5. Power semigroups.

Finally we take up here finite power semigroups as the simplest example of one-idempotent semigroups. Generally S is called a power semigroup if it is generated by only one element a of S, that is, S is composed of powers of a:

$$S=\{a, a^2, a^3, \cdots, a^n \cdots\}.$$

In particular, if S is finite, then some elements appear infinitely many times in this power sequence.

Let n be the d-order of S, λ_0 be the minimum of positive integers λ which have λ' greater than λ such that $a^\lambda = a^{\lambda'}$, and μ_0 be the minimum of positive integers μ which satisfy $a^{\lambda_0}=a^\mu$ where $\mu > \lambda_0$[12]. Then we see that $\mu_0=n+1$. Poole termed this λ_0 "the order", but here we call it the "origin" of S not to confuse with the orders already defined.

It follows that $a^\lambda \neq a^{2\lambda}$ for $\lambda < \lambda_0$ and $a^\lambda = a^\kappa$ for $\lambda, \kappa \geq \lambda_0$ if and only if $\lambda \equiv \kappa$ (mod. $\mu_0-\lambda_0$). Then the following theorem is easily proved.

Theorem 7. *A finite power semigroup S is one-idempotent and commutative, and the set*

$$a^{\lambda_0}, a^{\lambda_0+1}, \cdots, a^{\mu_0-1}$$

forms the greatest group of S, which is cyclic.

Now, let S and S' be two power semigroups with d-orders n, n', and with the origins λ_0, λ_0' respectively. Clearly S is isomorphic with S' if and only if $n=n'$ and $\lambda_0=\lambda_0'$. While the d-order n is fixed, only the origin determines the types of power semigroups.

Theorem 8. *The d-order and the origin characterize a finite power semi-*

12) See [1] or [2].

group. It follows from this that we have n types of non-isomorphic power semigroups of d-order n.

In the end of this paper, we shall give the following theorem referring to power zero semigroups.

Theorem 9. *If S is a zero-semigroup with d-order n and with v-order n−1, then S is a power semigroup.*

Proof. Theorem 6 makes it possible to put all elements of S in order[13]

$$a_1, a_2, \cdots, a_n$$

such that $SS_i \subset S_{i-1}$ and $S_iS \subset S_{i-1}$ where $S_i = \{a_1, \cdots, a_i\}$.

We may assume that $S = S_n$, $S^2 = S_{n-1}$. Now we shall prove that

$$a_i = a_{i+1}a_n$$

under the supposition $a_\lambda = a_{\lambda+1}a_n$ $(\lambda = i+1, i+2, \cdots, n-1)$.

By $SS_i \subset S_{i-1}$, and $S_iS \subset S_{i-1}$, we get easily $a_i \in (S-S_i)^2$, in other words

$$a_i \in (S-S_i)a_{i+1} \cup (S-S_i)a_{i+2} \cup \cdots \cup (S-S_i)a_n$$

or

$$a_i \in (S-S_i)a_n\,.\text{[14]}$$

From the assumption of induction, it follows that

$$a_i = a_{i+1}a_n\,.$$

On the other hand, by $SS_{n-1} \subset S_{n-2}$ and $S_{n-1}S \subset S_{n-2}$, we get

$$a_{n-1} \in SS-(SS_{n-1} \cup S_{n-1}S), \text{ that is, } a_{n-1} = a_n^2\,.$$

Thus every element of S is proved to be represented as a power of a_n.

Addendum.

As the corollaries of Theorem 6, 6′, we add the following two.

Corollary. *A zero-semigroup S of d-order n* $(n>2)$ *is homomorphic on a zero-semigroup of d-order* $n-i$, $1 \leqq i \leqq n-1$.

Proof. S_{i+1} mentioned in Theorem 6 is an ideal. It is sufficient to consider the difference semigroups of S modulo S_{i+1}.

Corollary. *A one-idempotent semigroup S of d-order n, and of g-order k is homomorphic on a zero-semigroup of d-order* $n-i$, $k-1 \leqq i \leqq n-1$.

---

13) Of course, a_1 is a zero, and a_2 is an annihilator distinct from zero.

14) For, $a_\lambda = a_{\lambda+1}a_n$ $(\lambda = i+1, i+2, \cdots, n-1)$.

The proofs of some theorems in this paper have been much improved in my paper to appear: "On compact one-idempotent semigroups."

Bibliography

[1] Suschkewitch, A., Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit, Math. Ann. 99. (1928) 30–50.

[2] Rees, D., On semigroups, Proc. Cambridge Phil. soc. vol. 36. (1940) 387–400.