EMBEDDING ANY SEMIGROUP IN A $\mathfrak{D}$-SIMPLE SEMIGROUP[1]

BY

G. B. PRESTON

1. **Introduction.** A semigroup is said to be *simple* if it has no proper two-sided ideals. Let S be a semigroup and let $\mathfrak{L}$ and $\mathfrak{R}$ be the equivalences:

$$\mathfrak{L} = \{(a, b) : a, b \in S \text{ and } Sa \cup a = Sb \cup b\};$$
$$\mathfrak{R} = \{(a, b) : a, b \in S \text{ and } aS \cup a = bS \cup b\}.$$

Denote by $\circ$ the operation of composition, so that if $A \subset X \times Y$ and $B \subset Y \times Z$ then $A \circ B = \{(x, z) : (x, y) \in A \text{ and } (y, z) \in B \text{ for some } y\}$. Then the minimal equivalence on S containing both $\mathfrak{L}$ and $\mathfrak{R}$ is $\mathfrak{D} = \mathfrak{L} \circ \mathfrak{R} = \mathfrak{R} \circ \mathfrak{L}$ (J. A. Green [1]). A semigroup is said to be $\mathfrak{D}$-*simple* if it consists of a single $\mathfrak{D}$-class. A $\mathfrak{D}$-simple semigroup is necessarily simple, a completely simple semigroup is $\mathfrak{D}$-simple, but in general a simple semigroup is not $\mathfrak{D}$-simple (see [1] and also §2 below). A semigroup is said to be *regular* if $a \in aSa$ for each a in S. If S is $\mathfrak{D}$-simple then, as shown by D. D. Miller and A. H. Clifford [2], S is regular if and only if S contains an idempotent. In particular, therefore, a $\mathfrak{D}$-simple semigroup with an identity is necessarily regular. A regular simple semigroup is not necessarily $\mathfrak{D}$-simple (see §2).

A recent result of R. H. Bruck [3, II, Theorem 8.3, p. 48] shows that any semigroup S can be embedded in a simple semigroup T, say, with identity. I show below that the simple semigroup T constructed by Bruck is $\mathfrak{D}$-simple if and only if S both has an identity and is $\mathfrak{D}$-simple. The main result of this paper is the following theorem: *any semigroup can be enbedded in a* (*necessarily regular*) $\mathfrak{D}$-*simple semigroup with an identity*. As a preliminary to the proof of this theorem we obtain (§3) a characterization of the $\mathfrak{D}$-classes of the semigroup of all mappings of a set into itself.

2. **The construction of R. H. Bruck.** Let S be a semigroup. If S has an identity element e, say, write $S = S^1$. If S has no identity element then, by the adjunction of a single element e, say, to S, we can embed S in a semigroup S^1 with identity. In either case S^1 is a semigroup with e as identity. Let N denote the set of non-negative integers. Let T be the set product $N \times S^1 \times N$ and define a product in T by the rule:

$$(m, s, n)(m', s', n') = (m + [m' - n], f(n - m'; s, s'), n' + [n - m']),$$

Presented to the Society, November 30, 1957 under the title *An embedding theorem for semigroups*; received by the editors July 25, 1958.

(1) This work was supported by the National Science Foundation grant to Tulane University.

where for any integer x,

$$[x] = x \text{ if } x \geqq 0; \qquad [x] = 0 \text{ if } x < 0;$$

and

$$f(x; s, s') = s, ss' \text{ or } s' \text{ according as } x > 0, x = 0 \text{ or } x < 0.$$

Then Bruck shows that with this product T becomes a simple semigroup, with $(0, e, 0)$ as its identity, in which S is embedded.

We now prove the result claimed in the introduction: *T is $\mathfrak{D}$-simple if and only if S has an identity and is $\mathfrak{D}$-simple.*

Firstly suppose that S has an identity and is $\mathfrak{D}$-simple so that S^1 is $\mathfrak{D}$-simple. Let (m, s, n) and (m', s', n') be any two elements of T. Since S^1 is $\mathfrak{D}$-simple there exists s'' in S^1 such that $s\mathfrak{L}s''\mathfrak{R}s'$. Hence, since S^1 has an identity, there exist x, y, u, v in S^1 such that $xs=s''$, $ys''=s$, $s''u=s'$ and $s'v=s''$. Then it may be verified that $(m', x, m)(m, s, n)=(m', s'', n)$ and $(m, y, m')(m', s'', n)=(m, s, n)$ so that $(m, s, n)\mathfrak{L}(m', s'', n)$. Similarly we have that $(m', s'', n)(n, u, n')=(m', s', n')$ and $(m', s', n')(n', v, n)=(m', s'', n)$ so that $(m', s'', n)\mathfrak{R}(m', s', n')$. Thus $(m, s, n)\mathfrak{L}(m', s'', n)\mathfrak{R}(m', s', n')$ and so $(m, s, n)\mathfrak{D}(m', s', n')$; and this proves that T is $\mathfrak{D}$-simple.

Conversely suppose that T is $\mathfrak{D}$-simple. For any s, s' in S^1 it follows, in particular, that $(0, s, 0)\mathfrak{D}(0, s', 0)$. Thus there exists an element (m, s'', n) in T such that $(0, s, 0)\mathfrak{L}(m, s'', n)\mathfrak{R}(0, s', 0)$. We will show that this implies that $s\mathfrak{L}s''\mathfrak{R}s'$.

Since $(0, s, 0)\mathfrak{L}(m, s'', n)$ there exist (p, x, q) and (p', y, q') in T such that $(p, x, q)(0, s, 0)=(m, s'', n)$ and $(p', y, q')(m, s'', n)=(0, s, 0)$. Thus

$$(p + [-q], f(q; x, s), [q]) = (m, s'', n)$$

and

$$(p' + [m - q'], f(q' - m; y, s''), n + [q' - m]) = (0, s, 0).$$

The second equation implies that $n=0$ and it then follows from the first equation that $q=0$. Hence $f(q; x, s)=xs$ and so from the first equation we have $xs=s''$. Again the second equation gives $[q'-m]=0$ and $[m-q']=0$ and these together imply that $q'=m$. Hence $f(q'-m; y, s'')=ys''$ and we have $ys''=s$. Thus $xs=s''$ and $ys''=s$ i.e. $s\mathfrak{L}s''$. By a similar argument we deduce that also $s''\mathfrak{R}s'$. Hence we have $s\mathfrak{D}s'$; and this shows that S^1 is $\mathfrak{D}$-simple.

It now follows that $S=S^1$. For if $S\neq S^1$ then the identity element e of S^1 is not $\mathfrak{D}$-equivalent to any element of S and so S^1 could not be $\mathfrak{D}$-simple. This completes the proof of our assertion.

Let S be regular but not $\mathfrak{D}$-simple. Then T is regular. For let $(m, a, n)\in T$. The regularity of S implies that S^1 is regular and hence there exists an x in S^1 such that $axa=a$. Then $(m, a, n)(n, x, m)(m, a, n)=(m, a, n)$ which shows that T is regular. Thus T is a simple regular semigroup which is not $\mathfrak{D}$-simple: which proves an assertion made earlier.

3. **Determination of the $\mathfrak{D}$-classes of the semigroup of all mappings of a set into itself.** Let $\Sigma(=\Sigma(A))$ be the semigroup of all single-valued mappings of A into A, combined under composition. The composition of the mapping α with the mapping β is the mapping obtained by following α by β (we write operators or mappings on the right). Regarding a mapping α of A into A as a subset of $A\times A$, namely the subset $\{(a, a\alpha): a\in A\}$, then this operation of composition is the same as that defined earlier in the introduction. It will be convenient in what follows to write sometimes $\alpha\beta$ and sometimes $\alpha\circ\beta$ for the composition of the mapping α with the mapping β. If $\alpha\subset A\times B$ then α^{-1} denotes the set $\{(x, y): (y, x)\in\alpha\}$; if $C\subset B$ then $C\alpha^{-1}$ denotes the set $\{x: (x, y)\in\alpha, y\in C\}$.

Since Σ has an identity element, namely the identical mapping of A onto A, two elements α, β in Σ are $\mathfrak{L}$-equivalent if and only if there exist γ, δ in Σ such that $\gamma\alpha=\beta$ and $\delta\beta=\alpha$. A similar comment applies to $\mathfrak{R}$-equivalent elements. We now give two lemmas which determine the $\mathfrak{L}$-classes and the $\mathfrak{R}$-classes of Σ.

LEMMA 1. *If $\alpha, \beta\in\Sigma$, then $(\alpha, \beta)\in\mathfrak{L}$ if and only if $A\alpha=A\beta$.*

Proof. If $(\alpha, \beta)\in\mathfrak{L}$ then there exist γ, δ in Σ such that $\gamma\alpha=\beta$ and $\delta\beta=\alpha$. Hence $A\beta=A\gamma\alpha\subset A\alpha$ and $A\alpha=A\delta\beta\subset A\beta$. Thus if $(\alpha, \beta)\in\mathfrak{L}$ then $A\alpha=A\beta$.

Conversely suppose that $A\alpha=A\beta$. Define the mapping γ of A into A as follows: for each element b in $A\beta$ let γ map the elements of the set $b\beta^{-1}$ onto a single element in $b\alpha^{-1}$. Then $\gamma\alpha=\beta$. Similarly there exists δ in Σ such that $\delta\beta=\alpha$. Thus $(\alpha, \beta)\in\mathfrak{L}$.

LEMMA 2. *If $\alpha, \beta\in\Sigma$ then $(\alpha, \beta)\in\mathfrak{R}$ if and only if $\alpha\circ\alpha^{-1}=\beta\circ\beta^{-1}$.*

Proof. If $(\alpha, \beta)\in\mathfrak{R}$ then there exist γ, δ in Σ such that $\alpha\gamma=\beta$ and $\beta\delta=\alpha$. Hence $\alpha\circ\alpha^{-1}=(\beta\delta)\circ(\beta\delta)^{-1}=\beta\circ(\delta\circ\delta^{-1})\circ\beta^{-1}\supset\beta\circ\beta^{-1}$; similarly, $\beta\circ\beta^{-1}\supset\alpha\circ\alpha^{-1}$. Hence $\alpha\circ\alpha^{-1}=\beta\circ\beta^{-1}$.

Conversely suppose that $\alpha\circ\alpha^{-1}=\beta\circ\beta^{-1}$. Then we may define a mapping γ as follows. Let γ map $A\backslash A\alpha$ identically and for b in $A\alpha$ let γ map b onto $(b\alpha^{-1})\beta$. The condition $\alpha\circ\alpha^{-1}=\beta\circ\beta^{-1}$ implies that $(b\alpha^{-1})\beta$ is a single element, for $\alpha\circ\alpha^{-1}$ is the equivalence relation on A determined canonically by α: $(x, y)\in\alpha\circ\alpha^{-1}$ if and only if $x\alpha=y\alpha$. Thus $\alpha\gamma=\beta$. Similarly there exists δ in Σ such that $\beta\delta=\alpha$. Thus $(\alpha, \beta)\in\mathfrak{R}$.

Using these lemmas we now easily have the following determination of the $\mathfrak{D}$-classes of Σ. Denote by $|X|$ the cardinal of a set X.

THEOREM 1. *Let Σ be the semigroup of all mappings of the set A into A combined under composition. Then α, β in Σ are $\mathfrak{D}$-equivalent if and only if $|A\alpha|=|A\beta|$.*

Proof. We know, since $\mathfrak{D}=\mathfrak{L}\circ\mathfrak{R}=\mathfrak{R}\circ\mathfrak{L}$, that $(\alpha, \beta)\in\mathfrak{D}$ if and only if there exists γ in Σ such that $(\alpha, \gamma)\in\mathfrak{L}$ and $(\gamma, \beta)\in\mathfrak{R}$. By Lemmas 1 and 2 this is equivalent to the existence of a mapping γ in Σ such that $A\alpha = A\gamma$ and $\gamma \circ \gamma^{-1} = \beta \circ \beta^{-1}$.

Consequently, denoting by A/ρ the quotient set determined by the equivalence ρ on A, if α is $\mathfrak{D}$-equivalent to β, then $|A\alpha| = |A\gamma| = |A/(\gamma \circ \gamma^{-1})| = |A/(\beta \circ \beta^{-1})| = |A\beta|$, so that $|A\alpha| = |A\beta|$.

Conversely, suppose that $|A\alpha| = |A\beta|$. Denote by ρ the equivalence $\beta \circ \beta^{-1}$ on A. Since $|A\beta| = |A/\rho|$, we have $|A/\rho| = |A\alpha|$. Let δ be any (1, 1)-mapping of A/ρ onto $A\alpha$. Then let γ be the mapping of A into A which maps the elements in each ρ-class onto the image of the ρ-class under δ. Then $\gamma \circ \gamma^{-1} = \rho = \beta \circ \beta^{-1}$ and $A\gamma = A\alpha$. Thus $(\alpha, \beta) \in \mathfrak{D}$; and this completes the proof of the theorem.

4. **The embedding theorem.** If S is a semigroup with an identity then it is easily verified that S is $\mathfrak{D}$-simple if and only if for any two elements a, b in S there exist elements s, t, u, v in S such that $as = ub$, $ast = a$ and $vub = b$.

To embed an arbitrary semigroup S in a $\mathfrak{D}$-simple semigroup we can clearly suppose, without loss of generality, that S contains an identity element. The first stage in our construction is to embed S in a semigroup $S(1)$, say, with the same identity element as S and such that for each pair of elements a, b in S there exist elements s, t, u, v in $S(1)$ such that $as = ub$, $ast = a$ and $vub = b$.

Let B be a set of elements disjoint from S and such that if $|S|$ is finite then $|B|$ is countably infinite, whilst if $|S|$ is infinite then $|B| = |S|$. Let $A = B \cup S$ and let $\Sigma = \Sigma(A)$, the semigroup of all mappings of A into A. Each element s in S then determines an element ρ_s in Σ defined thus:

$$x\rho_s = \begin{cases} xs, & \text{if } x \in S, \\ x, & \text{if } x \in B. \end{cases}$$

We easily verify, since by assumption S contains an identity element, that the mapping $s \rightarrow \rho_s$ embeds S isomorphically into Σ and that the identity element of S is mapped onto the identity element of Σ.

Now, for each s in S, $|A\rho_s| \geqq |B| = |A|$, and hence $|A\rho_s| = |A|$. Hence, by Theorem 1, all the elements ρ_s of Σ belong to the same $\mathfrak{D}$-class in Σ. Thus for each pair of elements s, t in S we may select a set of four elements α, β, ξ, η in Σ such that $\rho_s\alpha = \xi\rho_t$, $\rho_s\alpha\beta = \rho_s$ and $\eta\xi\rho_t = \rho_t$. For each pair of elements s, t in S select a definite set of four such elements and let P denote the set of all such elements so selected. Let $S(1)$ be the subsemigroup of Σ generated by $P \cup \{\rho_s : s \in S\}$. Then, regarding S as identified with its image in $S(1)$ under the mapping $s \rightarrow \rho_s$, we have embedded S in a semigroup $S(1)$ with the properties we required, and the first stage of the construction is completed.

Now construct $S(2)$ from $S(1)$ in exactly the same way as $S(1)$ was constructed from S. Similarly we construct $S(n+1)$ from $S(n)$ for any integer $n \geqq 1$. Let $T = \bigcup_{n=1}^{\infty} S(n)$.

Then T contains an identity element, viz. the common identity of all the

$S(n)$. Further for any a, b in T there exists an integer n such that $a, b \in S(n)$ and then there necessarily exist s, t, u, v in $S(n+1)$, and hence in T, such that $as = ub$, $ast = a$ and $vub = b$. Thus, in view of a remark made earlier, T is $\mathfrak{D}$-simple and we have proved the following theorem.

THEOREM 2. *Any semigroup can be embedded in a (necessarily regular) $\mathfrak{D}$-simple semigroup with identity.*

We note finally that our construction is such that if S is infinite then $|T| = |S|$ and that if S is finite then T is at most countably infinite.

ACKNOWLEDGMENT. In the author's original proof of Theorem 2 $S(1)$ was constructed as a free semigroup subject to certain relations. In a letter to the author (February, 1958) Dr. M. P. Schützenberger suggested that it could probably be shown that when A is an infinite set then the subset $\Omega(A)$ of $\Sigma(A)$ consisting of all those mappings α such that (i) $|A| = |A\alpha|$ and (ii) for all b in $A\alpha$, $|b\alpha^{-1}| < |A|$, formed a $\mathfrak{D}$-simple subsemigroup of Σ. In fact Ω is a semigroup if and only if $|A|$ is a regular cardinal and when it is a semigroup it is $\mathfrak{D}$-simple. Then, as Dr. Schützenberger suggested, the proof of Theorem 2 can be completed in one step by the mapping $s \to \rho_s$ of the previous section which now embeds S in $\Omega(A)$ if we choose B such that $|B| > |S|$. The referee suggested yet a further proof of Theorem 2. The proof given in the paper results from a combination of the referee's proof with the author's proof of Dr. Schützenberger's conjecture.

REFERENCES

1. J. A. Green, *On the structure of semigroups*, Ann. of Math. vol. 54 (1951) pp. 163–172.

2. D. D. Miller and A. H. Clifford, *Regular $\mathfrak{D}$-classes in semigroups*, Trans. Amer. Math. Soc. vol. 82 (1956) pp. 270–280.

3. R. H. Bruck, *A survey of binary systems*, Ergebnisse der Math., Neue Folge, vol. 20, Springer, 1958.

ROYAL MILITARY COLLEGE OF SCIENCE,
SHRIVENHAM, ENGLAND