CONGRUENCES ON A BISIMPLE ω-SEMIGROUP

by W. D. MUNN and N. R. REILLY

(Received 10 August, 1965)

In a semigroup S the set E of idempotents is partially ordered by the rule that $e \leqq f$ if and only if $ef = e = fe$. We say that S is an *ω-semigroup* if $E = \{e_i\colon\ i = 0, 1, 2, \ldots\}$, where

$$e_0 > e_1 > e_2 > \ldots .$$

Bisimple ω-semigroups have been classified in [**10**]. From a group G and an endomorphism α of G a bisimple ω-semigroup $S(G, \alpha)$ can be constructed by a process described below in § 1; moreover, any bisimple ω-semigroup is isomorphic to one of this type.

The present paper is concerned with congruences on $S = S(G, \alpha)$ and with homomorphic images of S. It is shown that a congruence ρ on S is either an idempotent-separating congruence or a group congruence (that is, S/ρ is a group). The idempotent-separating congruences are in a natural one-to-one correspondence with the α-admissible normal subgroups of G and the maximal such congruence is just Green's equivalence, $\mathscr{H}$. We determine the nature of each of the quotient semigroups $S/\mathscr{H}$, $S/(\sigma \cap \mathscr{H})$, S/σ and $S/(\sigma \vee \mathscr{H})$, where σ denotes the minimum group congruence on S. The structure of S/σ (the maximum group homomorphic image of S) is described in terms of the direct α-limit of G.

Finally, a sufficient condition is given for the lattice of congruences on S to be modular.

1. Throughout this paper we shall adhere to the following convention: N will denote the set of all non-negative integers, G will denote a group and α will denote an endomorphism of G. We shall use the symbol 1 for the identity of G; from the context this will always be distinguishable from the integer 1.

The bicyclic semigroup [**1**, p. 43] will be denoted by B. It can be considered as the set $N \times N$ endowed with the multiplication

$$(m, n)(p, q) = (m+p-r, n+q-r),$$

where $r = \min\{n, p\}$. This can be generalised as follows. Let $S(G, \alpha)$ denote the set of all ordered triples $(m\,;\ g;\ n)$, where $m, n \in N$ and $g \in G$. Define a multiplication on $S(G, \alpha)$ by the rule that

$$(m;\ g;\ n)(p;\ h;\ q) = (m+p-r;\ g\alpha^{p-r}h\alpha^{n-r};\ n+q-r), \tag{1}$$

where $r = \min\{n, p\}$. We interpret α^0 as the identity automorphism of G. Then, as was shown in [**10**], $S(G, \alpha)$ is a bisimple ω-semigroup and any bisimple ω-semigroup is isomorphic to a semigroup of the type $S(G, \alpha)$. The bicyclic semigroup is obtained by taking $G = \{1\}$.

For each n in N, write

$$e_n = (n;\ 1;\ n).$$

The elements e_n are the idempotents of $S(G, \alpha)$ and we have that

$$e_0 > e_1 > e_2 > \ldots .$$

https://doi.org/10.1017/S2040618500035413 Published online by Cambridge University Press

It is almost immediate that $S(G, \alpha)$ is an inverse semigroup [1, § 1.9] with identity e_0 and that

$$(m;\ g;\ n)^{-1} = (n;\ g^{-1};\ m).$$

From (1) it is also easy to show that the equivalence $\mathscr{H}$ [1, § 2.1] is given by

$$((m;\ g;\ n), (p;\ h;\ q)) \in \mathscr{H} \Leftrightarrow m = p \quad \text{and} \quad n = q;$$

this result will be used frequently. In particular, the group of units of $S(G, \alpha)$ (the $\mathscr{H}$-class containing e_0) is the subset

$$U = \{(0;\ g;\ 0) : g \in G\}.$$

Proofs that are of a straightforward computational nature (using, for example, the law of multiplication (1)) will often be omitted.

Let ρ be an equivalence on a set S. We denote the ρ-class of S containing the element x of S by $x\rho$. Now let S be a semigroup. Then ρ is a congruence if and only if

$$(x, y) \in \rho \Rightarrow (ax, ay) \in \rho \quad \text{and} \quad (xa, ya) \in \rho$$

for all a in S. The basic properties of congruences are described in [1, § 1.5]. In particular, if ρ and τ are congruences on S then the congruences $\rho \cap \tau$ and $\rho \vee \tau$ have an obvious set-theoretic meaning within $S \times S$ and the set of all congruences on S forms a lattice with respect to inclusion in $S \times S$.

If $\rho \subseteq \tau$ then we can define a congruence τ/ρ on S/ρ by the rule that

$$(x\rho, y\rho) \in \tau/\rho \Leftrightarrow (x, y) \in \tau;$$

furthermore, $(S/\rho)/(\tau/\rho) \cong S/\tau$. Conversely, if τ^* is any congruence on S/ρ then there exists a congruence τ on S containing ρ and such that $\tau^* = \tau/\rho$.

We call a congruence ρ on S a *group congruence* if S/ρ is a group. From the preceding paragraph we see that if τ is any congruence on S containing a group congruence then τ is itself a group congruence. The following result provides a characterisation of the minimum group congruence σ on an inverse semigroup [7, Theorem 1].

LEMMA 1.1. *Let S be an inverse semigroup and let a relation σ be defined on S by the rule that $(x, y) \in \sigma$ if and only if $ex = ey$ for some idempotent e in S (or, equivalently, if and only if $xf = yf$ for some idempotent f). Then σ is a group congruence on S. Furthermore, a congruence ρ on S is a group congruence if and only if $\sigma \subseteq \rho$.*

A congruence λ on a semigroup S is said to be *idempotent-separating* if no two distinct idempotents of S lie in the same λ-class. Clearly, if S has more than one idempotent, then an idempotent-separating congruence cannot also be a group congruence. Howie [3] has shown that on an inverse semigroup S there exists a maximum idempotent-separating congruence μ; thus a congruence λ on S is idempotent-separating if and only if $\lambda \subseteq \mu$. Moreover, μ can be characterised as the largest congruence contained in $\mathscr{H}$. (See also [6].) Hence if $\mathscr{H}$ itself is a congruence then $\mathscr{H} = \mu$. This is the case for a bisimple ω-semigroup, as we now show.

LEMMA 1.2. *Let $S = S(G, \alpha)$. Then $\mathscr{H}$ is a congruence on S and $S/\mathscr{H} \cong B$.*

N

Proof. The mapping θ of S onto B defined by $(m;\ g;\ n)\theta = (m, n)$ is a homomorphism. Further, $((m;\ g;\ n), (p;\ h;\ q)) \in \mathscr{H}$ if and only if $(m, n) = (p, q)$; hence $\theta \circ \theta^{-1} = \mathscr{H}$ and the result follows.

Remark. More generally, if S is an inverse semigroup whose semilattice of idempotents E is such that each principal ideal of E is well-ordered under the converse of the natural ordering, then $\mathscr{H}$ is a congruence on S [**8**, Theorem 3.2].

We now establish a fundamental property of congruences on a bisimple ω-semigroup.

THEOREM 1.3. *A congruence on $S(G, \alpha)$ is either an idempotent-separating congruence or a group congruence.*

Proof. Let $S = S(G, \alpha)$ and let ρ be a congruence on S. Suppose that ρ is not idempotent-separating. Then $(e_m, e_{m+k}) \in \rho$ for some m, k in N, with $k > 0$. We shall show that all the idempotents of S are ρ-equivalent. First let $x = (0;\ 1;\ m)$. Then $xe_m x^{-1} = e_0$ and $xe_{m+k}x^{-1} = e_k$. Hence $(e_0, e_k) \in \rho$. Since $e_0 e_1 = e_1$ and $e_k e_1 = e_k$ it follows that $(e_1, e_k) \in \rho$. Thus $(e_0, e_1) \in \rho$. Now suppose that we have shown that $(e_0, e_n) \in \rho$ for some positive integer n. Let $y = (n;\ 1;\ 0)$. Then $ye_0 y^{-1} = e_n$ and $ye_1 y^{-1} = e_{n+1}$, from which we deduce that $(e_n, e_{n+1}) \in \rho$. Hence $(e_0, e_{n+1}) \in \rho$. Thus, by induction on n, all the idempotents of S lie in the same ρ-class, I, say. Let $a \in S$. Then $I \,.\, a\rho = (aa^{-1})\rho \,.\, a\rho \subseteq a\rho$; also $a^{-1}\rho \,.\, a\rho \subseteq (a^{-1}a)\rho = I$. Hence S/ρ is a group. This completes the proof.

Let Λ denote the lattice of congruences on $S(G, \alpha)$. Then this theorem shows that Λ is the disjoint union of the sublattices $\Lambda_{IS} = \{\lambda \in \Lambda : \lambda \subseteq \mathscr{H}\}$ and $\Lambda_G = \{\lambda \in \Lambda : \sigma \subseteq \lambda\}$ consisting of all idempotent-separating congruences and of all group congruences respectively.

2. For any congruence λ on $S = S(G, \alpha)$ we define a subset A_λ of G as follows:

$$A_\lambda = \{g \in G : ((0;\ g;\ 0), e_0) \in \lambda\}.$$

Note that $A_\lambda = A_{\lambda \cap \mathscr{H}}$, since the $\mathscr{H}$-class containing e_0 is $U = \{(0;\ g;\ 0) \in S : g \in G\}$. It will be convenient to express properties of congruences on S in terms of the sets A_λ.

LEMMA 2.1. *For any congruence λ on $S(G, \alpha)$, A_λ is an α-admissible normal subgroup of G.*

Proof. Let $\lambda_0 = \lambda \cap (U \times U)$. Then λ_0 is a congruence on U and so, since $e_0\lambda_0$ is a normal subgroup of U and is the image of A_λ under the isomorphism $g \to (0;\ g;\ 0)$ from G to U, A_λ is a normal subgroup of G.

Now let $g \in A_\lambda$. Write $x = (0;\ g;\ 0)$ and $z = (0;\ 1;\ 1)$. Then $(x, e_0) \in \lambda$ and so $(zxz^{-1}, ze_0z^{-1}) \in \lambda$. But $zxz^{-1} = (0;\ g\alpha;\ 0)$ and $ze_0z^{-1} = e_0$. Hence $g\alpha \in A_\lambda$. Thus A_λ is α-admissible.

Let ker a^k denote the kernel of the endomorphism α^k for $k = 1, 2, 3, \ldots$.

LEMMA 2.2.

$$A_{\sigma \cap \mathscr{H}} = A_\sigma = \bigcup_{k=1}^{\infty} \ker \alpha^k.$$

Proof. Let $g \in A_\sigma$. Then $((0;\ g;\ 0), e_0) \in \sigma$ and so, by Lemma 1.1, $e_m(0;\ g;\ 0) = e_m e_0$ for some m; that is, $(m;\ g\alpha^m;\ m) = e_m$. Thus $g\alpha^m = 1$ and so

$$g \in \bigcup_{k=1}^{\infty} \ker \alpha^k.$$

https://doi.org/10.1017/S2040618500035413 Published online by Cambridge University Press

Conversely, let

$$g \in \bigcup_{k=1}^{\infty} \ker \alpha^k.$$

Then $g\alpha^m = 1$ for some m and so $e_m(0;\ g;\ 0) = e_m e_0$. Hence $((0;\ g;\ 0), e_0) \in \sigma$; that is, $g \in A_\sigma$. Hence

$$A_\sigma = \bigcup_{k=1}^{\infty} \ker \alpha^k,$$

and, by an earlier remark, $A_{\sigma \cap \mathscr{H}} = A_\sigma$.

We now consider idempotent-separating congruences. These can be characterised as follows.

LEMMA 2.3.

(i) *Let λ be an idempotent-separating congruence on $S(G, \alpha)$. Then*

$$((m;\ g;\ n), (p;\ h;\ q)) \in \lambda \Leftrightarrow m = p, \quad n = q \quad \text{and} \quad gh^{-1} \in A_\lambda.$$

(ii) *For any α-admissible normal subgroup A of G there exists an idempotent-separating congruence λ on $S(G, \alpha)$ such that $A = A_\lambda$.*

The proof is omitted.

Remark. From Lemmas 2.2 and 2.3 we see that $\sigma \cap \mathscr{H}$ is the identical congruence on $S = S(G, \alpha)$ if and only if

$$\bigcup_{k=1}^{\infty} \ker \alpha^k = \{1\},$$

that is, if and only if α is one-to-one. It can be shown that this holds in turn if and only if the set E of idempotents of S is unitary in S. This result should be compared with [4, Theorem 3.9].

Let A be an α-admissible normal subgroup of G. We define a mapping α/A of G/A into itself by the rule that $(Ag)(\alpha/A) = A(g\alpha)$ for all g in G. That this is well-defined is a consequence of the α-admissibility of A. It is immediate that α/A is an endomorphism; moreover, if we define α^k/A on G/A in a similar way, then $(\alpha/A)^k = \alpha^k/A$ for any positive integer k.

THEOREM 2.4. *Let λ be an idempotent-separating congruence on $S = S(G, \alpha)$. Then $S/\lambda \cong S(G/A_\lambda, \alpha/A_\lambda)$.*

Proof. Consider the mapping θ of S onto $S(G/A_\lambda, \alpha/A_\alpha)$ defined by

$$(m;\ g;\ n)\theta = (m;\ A_\lambda g;\ n).$$

Since

$$A_\lambda(g\alpha^r \,.\, h\alpha^s) = (A_\lambda g)(\alpha/A_\lambda)^r \,.\, (A_\lambda h)(\alpha/A_\lambda)^s$$

$(g, h \in G;\ r, s \in N)$, it follows that θ is a homomorphism. Also, $(m;\ g;\ n)\theta = (p;\ h;\ q)\theta$ if and only if $m = p$, $n = q$ and $A_\lambda g = A_\lambda h$. By Lemma 2.3 (i) these equalities hold if and only if $((m;\ g;\ n), (p;\ h;\ q)) \in \lambda$. Hence $\theta \circ \theta^{-1} = \lambda$, which gives the required result.

https://doi.org/10.1017/S2040618500035413 Published online by Cambridge University Press

COROLLARY 2.5. *Let $S = S(G, \alpha)$ and let*

$$K = \bigcup_{k=1}^{\infty} \ker \alpha^k.$$

Then $S/(\sigma \cap \mathscr{H}) \cong S(G/K, \alpha/K)$.

This follows from Lemma 2.2.

A result related to that of Theorem 2.4 can be obtained by a straightforward generalisation of [**10**, Theorem 4.1], making use of Theorem 1.3. Let α' be an endomorphism of a group G'. Then there exists a homomorphism of $S(G, \alpha)$ onto $S(G', \alpha')$ if and only if there exists a homomorphism θ of G onto G' and an element z of G' such that

$$\alpha\theta = \theta\alpha'\psi_z,$$

where ψ_z denotes the inner automorphism $x \to zxz^{-1}$ of G'. We omit the proof.

3. We now turn our attention to group congruences. The main aim of this section is to find the structure of the maximum group homomorphic image of $S(G, \alpha)$; this is achieved in Theorem 3.4.

Let us first define a relation ρ on $G \times N$ by the rule that

$$((a, i), (b, j)) \in \rho \Leftrightarrow a\alpha^{r-i} = b\alpha^{r-j}$$

for some $r \geqq i, j$ (and therefore for all sufficiently large r).

LEMMA 3.1. *ρ is an equivalence on $G \times N$. Further, the rule*

$$(a, i)\rho \,.\, (b, j)\rho = (a\alpha^{m-i}b\alpha^{m-j}, m)\rho,$$

where $m =$ max $\{i, j\}$, defines a binary operation on $(G \times N)/\rho$ with respect to which this set is a group.

The proof is omitted. We shall denote the group $(G \times N)/\rho$ so formed by G_α and call it the *direct α-limit* of G. For a discussion of direct limits of groups, see [**5**, § 7].

Clearly

$$(a, i)\rho = (a\alpha^n, i+n)\rho \tag{2}$$

for all n in N.

Next we define $\dot{\alpha} : G_\alpha \to G_\alpha$ by $(a, i)\rho\dot{\alpha} = (a\alpha, i)\rho$. The following result was suggested to us by A. H. Clifford.

LEMMA 3.2. *$\dot{\alpha}$ is an automorphism of G_α. For all p, q in N we have that*

$$(a, i)\rho\dot{\alpha}^{p-q} = (a\alpha^p, i+q)\rho.$$

Proof. By virtue of (2) we see that the mapping $\dot{\alpha}$ has a two-sided inverse $\dot{\alpha}^{-1}$ defined by $(a, i)\rho\dot{\alpha}^{-1} = (a, i+1)\rho$. To complete the proof that it is an automorphism we note that

$$\begin{aligned} [(a, i)\rho\dot{\alpha}][(b, j)\rho\dot{\alpha}] &= ((a\alpha)\alpha^{m-i}(b\alpha)\alpha^{m-j}, m)\rho, \quad \text{where } m = \max\{i, j\}, \\ &= (a\alpha^{m-i} \,.\, b\alpha^{m-j}, m)\rho\dot{\alpha} \\ &= [(a, i)\rho(b, j)\rho]\dot{\alpha}. \end{aligned}$$

https://doi.org/10.1017/S2040618500035413 Published online by Cambridge University Press

By induction on p we have that $(a, i)\rho\dot{\alpha}^p = (a\alpha^p, i)\rho$ for all p in N. Similarly, $(a, i)\rho\dot{\alpha}^{-q} = (a, i+q)\rho$ for all q in N and, combining these, we have that

$$(a, i)\rho\dot{\alpha}^{p-q} = (a\alpha^p, i+q)\rho$$

for all p, q in N. (Note that in the case $p = q$ this reduces to (2).)

For the remainder of this section the group of all integers under addition will be denoted by Z.

LEMMA 3.3. *Let H be a group and β an automorphism of H. Define a multiplication on the set $Z \times H$ by the rule that*

$$(i, a)(j, b) = (i+j, a\beta^j b).$$

Then, with respect to this operation, $Z \times H$ is a group.

Again we omit the proof. We shall denote the group so formed by $H \uparrow \beta$. This is a semi-direct product of H by Z [2, § 6.5].

The direct product of two semigroups P and Q will be denoted by $P \dot{\times} Q$. If β is an *inner* automorphism of H then $H \uparrow \beta \cong Z \dot{\times} H$. To see this, let β be the mapping $x \to h^{-1}xh$ determined by the element h of H; then the mapping $(i, a) \to (i, h^i a)$ of $H \uparrow \beta$ onto $Z \dot{\times} H$ is an isomorphism.

We now describe the maximum group homomorphic image of $S(G, \alpha)$.

THEOREM 3.4. *Let $S = S(G, \alpha)$. Then $S/\sigma \cong G_\alpha \uparrow \dot{\alpha}$.*

Proof. Define a mapping $\theta : S \to G_\alpha \uparrow \dot{\alpha}$ by the rule that

$$(m;\ g;\ n)\theta = (m-n, (g, n)\rho).$$

First we show that θ is surjective. Let $i \in Z$ and let $(g, n)\rho$ be any element of G_α ($g \in G$, $n \in N$). If $i \geqq 0$, then $(i, (g, n)\rho) = (i+n;\ g;\ n)\theta$. On the other hand, if $i < 0$, then, by (2),

$$(i, (g, n)\rho) = (i, (g\alpha^{-i}, n-i)\rho) = (n;\ g\alpha^{-i};\ n-i)\theta.$$

Now let $(m;\ g;\ n)$ and $(p;\ h;\ q)$ be any two elements of S. Then

$$\begin{aligned}
&(m;\ g;\ n)\theta(p;\ h;\ q)\theta \\
&\quad = (m-n, (g, n)\rho)(p-q, (h, q)\rho) \\
&\quad = (m-n+p-q, (g, n)\rho\dot{\alpha}^{p-q}(h, q)\rho) \\
&\quad = (m-n+p-q, (g\alpha^p, n+q)\rho(h, q)\rho), \quad \text{by Lemma 3.2,} \\
&\quad = (m-n+p-q, (g\alpha^p h\alpha^n, n+q)\rho) \\
&\quad = (m-n+p-q, (g\alpha^{p-r}h\alpha^{n-r}, n+q-r)\rho), \text{ by (2),} \quad \text{where } r = \min\{n, p\}, \\
&\quad = (m+p-r;\ g\alpha^{p-r}h\alpha^{n-r};\ n+q-r)\theta \\
&\quad = [(m;\ g;\ n)(p;\ h;\ q)]\theta.
\end{aligned}$$

https://doi.org/10.1017/S2040618500035413 Published online by Cambridge University Press

Thus θ is a homomorphism. Since $S\theta$ is a group and σ is the minimum group congruence on S, it follows that $\sigma \subseteq \theta \circ \theta^{-1}$.

To complete the proof we shall show that $\theta \circ \theta^{-1} \subseteq \sigma$. Let $(m;\ g;\ n)\theta = (p;\ h;\ q)\theta$. Then

$$(m-n, (g, n)\rho) = (p-q, (h, q)\rho).$$

Hence $m-n = p-q$ and $(g, n)\rho = (h, q)\rho$. From the latter equality we have that $g\alpha^{k-n} = h\alpha^{k-q}$ for some $k \geqq n, q$. Thus

$$(m;\ g;\ n)e_k = (m+k-n;\ g\alpha^{k-n};\ k) = (p+k-q;\ h\alpha^{k-q};\ k) = (p;\ h;\ q)e_k$$

and so, by Lemma 1.1, $((m;\ g;\ n), (p;\ h;\ q)) \in \sigma$. Hence $\theta \circ \theta^{-1} \subseteq \sigma$.

We have therefore shown that $\theta \circ \theta^{-1} = \sigma$ and so $S/\sigma \cong S\theta = G_\alpha \uparrow \dot{\alpha}$.

In certain cases G_α can be embedded in G and the structure of S/σ assumes a simpler form. We say that α is *stable* if, for some k, $\alpha \mid G\alpha^k$ is an automorphism of $G\alpha^k$. The smallest k for which this condition holds will be called the *index of stability* of α. Evidently α is stable if it is an automorphism of G. Also α is stable if it is *nilpotent*, that is, if $\alpha^n = \zeta$ (the zero endomorphism of G, defined by $g\zeta = 1$ for all g in G) for some n. Note that, if G is finite, then α is necessarily stable.

Let α be stable, with index of stability k. We prove that $G_\alpha \cong G\alpha^k$. Let $\beta = \alpha \mid G\alpha^k$ and let $\phi : G_\alpha \to G\alpha^k$ be defined by

$$(g, i)\rho\phi = g\alpha^k\beta^{-i}.$$

First, for any g in G we have that $(g\alpha^i, i)\rho\phi = g\alpha^{i+k}\beta^{-i} = g\alpha^k$ and so ϕ is surjective. Also, if $g\alpha^k\beta^{-i} = h\alpha^k\beta^{-j}$, then $g\alpha^{k+m-i} = h\alpha^{k+m-j}$, where $m = \max\{i, j\}$, and so $(g, i)\rho = (h, j)\rho$. This shows that ϕ is one-to-one. Moreover, for any elements $(g, i)\rho$ and $(h, j)\rho$ in G_α we have that

$$\begin{aligned}[(g, i)\rho(h, j)\rho]\phi &= (g\alpha^{m-i}h\alpha^{m-j}, m)\rho\phi, \quad \text{where } m = \max\{i, j\},\\ &= (g\alpha^{m-i}h\alpha^{m-j})\alpha^k\beta^{-m}\\ &= (g\alpha^k\beta^{-i})(h\alpha^k\beta^{-j}) = (g, i)\rho\phi(h, j)\rho\phi.\end{aligned}$$

It is easy to show that $\phi\beta = \dot{\alpha}\phi$ and from this it follows that the mapping $\psi : G_\alpha \uparrow \dot{\alpha} \to G\alpha^k \uparrow \beta$ defined by

$$(j, (g, i)\rho)\psi = (j, (g, i)\rho\phi) = (j, g\alpha^k\beta^{-i})$$

is an isomorphism. Thus we have

COROLLARY 3.5. *Let $S = S(G, \alpha)$, where α is stable with index of stability k. Let $\beta = \alpha \mid G\alpha^k$. Then*

$$S/\sigma \cong G\alpha^k \uparrow \beta.$$

A further specialisation gives the following two results.

COROLLARY 3.6. *If α is an automorphism, then $S/\sigma \cong G \uparrow \alpha$. In particular, if α is an inner automorphism, then $S/\sigma \cong Z \dot{\times} G$.*

It should be noted that, if α is an inner automorphism, then $S \cong B \dot{\times} G$ [**10**, Corollary 4.2].

COROLLARY 3.7. *If $\alpha^{k+1} = \alpha^k$ for some k, then $S/\sigma \cong Z \dot{\times} G\alpha^k$. In particular, if α is nilpotent, then $S/\sigma \cong Z$.*

We return now to the case in which no restrictions are placed on α. Since the group homomorphic images of $S = S(G, \alpha)$ are just the homomorphic images of $G_\alpha \uparrow \dot{\alpha}$, it follows that Z is one such image. The next theorem shows that this is determined by the congruence $\sigma \vee \mathscr{H}$.

LEMMA 3.8. *Let $S = S(G, \alpha)$. Then*

$$((m;\ g;\ n), (p;\ h;\ q)) \in \sigma \vee \mathscr{H} \Leftrightarrow m-n = p-q.$$

Proof. Let $x = (m;\ g;\ n)$ and $y = (p;\ h;\ q)$. First suppose that $(x, y) \in \sigma \vee \mathscr{H}$. Then, since $\sigma \vee \mathscr{H} = \sigma \circ \mathscr{H} \circ \sigma$ [**3**, Theorem 3.9], there exist elements a, b in S such that $(x, a) \in \sigma$, $(a, b) \in \mathscr{H}$ and $(b, y) \in \sigma$. Let $a = (m';\ g';\ n')$ and $b = (p';\ h';\ q')$. Since $(x, a) \in \sigma$, there exists an idempotent e_k such that $e_k x = e_k a$ (Lemma 1.1) and we can assume, without loss of generality, that $k \geqq m$, m'. Hence we have $k+n-m = k+n'-m'$ and so $m-n = m'-n'$. Similarly, since $(b, y) \in \sigma$, we have $p-q = p'-q'$. But $m' = p'$ and $n' = q'$, since $(a, b) \in \mathscr{H}$. Hence $m-n = p-q$.

Conversely, let x and y be such that $m-n = p-q$. We assume that $m \leqq p$. Then $e_p x = (p;\ g\alpha^{p-m};\ p+n-m) = (p;\ g\alpha^{p-m};\ q)$ and so $(e_p x, y) \in \mathscr{H}$. But $(x, e_p x) \in \sigma$, since e_p is an idempotent. Hence $(x, y) \in \sigma \circ \mathscr{H} \subseteq \sigma \vee \mathscr{H}$. This establishes the lemma.

THEOREM 3.9. *Let $S = S(G, \alpha)$. Then $S/(\sigma \vee \mathscr{H}) \cong Z$.*

Proof. Consider the mapping θ of S onto Z defined by $(m;\ g;\ n)\theta = m-n$. It is immediate from (1) that θ is a homomorphism. From Lemma 3.8 we have that

$$\theta \circ \theta^{-1} = \sigma \vee \mathscr{H}$$

and the required result follows.

4. We conclude with some further remarks on the lattice of congruences Λ on $S = S(G, \alpha)$. Let Λ_{IS} and Λ_G be defined as at the end of § 1; then $\Lambda_{IS} \cup \Lambda_G = \Lambda$ and $\Lambda_{IS} \cap \Lambda_G = \emptyset$.

Now Λ_G is modular, since it is isomorphic to the lattice of all congruences on the group S/σ. Also, Λ_{IS} is modular by [**6**, Theorem 3.2]. This can be proved directly as follows. Let $\mathscr{A}$ denote the set of all α-admissible normal subgroups of G. Since AA' and $A \cap A'$ lie in $\mathscr{A}$ for all A, A' in $\mathscr{A}$, it follows that $\mathscr{A}$ is a sublattice of the lattice of *all* normal subgroups of G. Hence $\mathscr{A}$ is modular. But from Lemma 2.3 (i) we have that

$$\lambda \subseteq \lambda' \Leftrightarrow A_\lambda \subseteq A_{\lambda'} \quad (\lambda, \lambda' \in \Lambda_{IS})$$

and so the mapping $\phi : \Lambda_{IS} \to \mathscr{A}$ given by $\lambda\phi = A_\lambda$—which is surjective, by Lemma 2.3 (ii)—is a lattice isomorphism.

It is natural to ask whether Λ itself is modular. A full discussion of this question is given in [**9**]; we shall confine ourselves here to obtaining a sufficient condition for modularity.

In general σ and $\mathscr{H}$ are incomparable. It can happen, however, that $\mathscr{H}$ is contained in σ. We now give a necessary and sufficient condition for this to hold.

LEMMA 4.1. *Let $S = S(G, \alpha)$. Then*

$$\mathscr{H} \subset \sigma \Leftrightarrow \bigcup_{k=1}^{\infty} \ker \alpha^k = G.$$

Proof. Write

$$K = \bigcup_{k=1}^{\infty} \ker \alpha^k.$$

First let $\mathscr{H} \subset \sigma$ and let $g \in G$. Then since $((0;\ g;\ 0), e_0) \in \mathscr{H}$ we have that $g \in A_\sigma$. But $A_\sigma = K$, by Lemma 2.2. Hence $G \subseteq K$ and so $G = K$.

Conversely, let $G = K$. Consider the $\mathscr{H}$-equivalent elements $x = (m;\ g;\ n)$ and $y = (m;\ h;\ n)$. Since $gh^{-1} \in K$ by hypothesis, there exists k such that $(gh^{-1})\alpha^k = 1$. Thus $g\alpha^k = h\alpha^k$. Then

$$e_{m+k}x = (m+k;\ g\alpha^k;\ n+k) = (m+k;\ h\alpha^k;\ n+k) = e_{m+k}y$$

and so $(x, y) \in \sigma$, by Lemma 1.1. Thus $\mathscr{H} \subseteq \sigma$; moreover, equality is impossible.

In particular, $\mathscr{H} \subset \sigma$ if α is nilpotent.

We note, in passing, that if

$$\bigcup_{k=1}^{\infty} \ker \alpha^k = G,$$

then $\sigma = \sigma \vee \mathscr{H}$ and, combining this with Theorem 3.9, we have another proof of the fact that if α is nilpotent, then $S/\sigma \cong Z$. (See Corollary 3.7.)

Finally, we have

THEOREM 4.2. *The lattice of congruences on $S(G, \alpha)$ is modular if*

$$\bigcup_{k=1}^{\infty} \ker \alpha^k = G.$$

In particular, this holds if α is nilpotent.

The result follows from Lemma 4.1 and the fact that Λ_{IS} and Λ_G are both modular.

REFERENCES

1. A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. I, Math. Surveys of the American Math, Soc. 7 (Providence, R.I., 1961).

2. M. Hall, Jr., *The theory of groups* (New York, 1959).

3. J. M. Howie, The maximum idempotent-separating congruence on an inverse semigroup, *Proc. Edinburgh Math. Soc.* **14** (1964), 71–79.

4. J. M. Howie and G. Lallement, Certain fundamental congruences on a regular semigroup, *Proc. Glasgow Math. Assoc.* **7** (1966), 145–159.

5. A. G. Kurosh, *The theory of groups*, Vol. 1 (English translation, New York, 1955).

6. G. Lallement, Congruences et équivalences de Green sur un demi-groupe régulier, *C. R. Acad. Sc. Paris* Série A **262** (1966), 613–616.

7. W. D. Munn, A class of irreducible matrix representations of an arbitrary inverse semigroup, *Proc. Glasgow Math. Assoc.* **5** (1961), 41–48.

8. W. D. Munn, Uniform semilattices and bisimple inverse semigroups, *Quarterly J. Math. Oxford* Ser. 2 (to appear).

9. W. D. Munn, The lattice of congruences on a bisimple ω-semigroup, *Proc. Roy. Soc. Edinburgh* (to appear).

10. N. R. Reilly, Bisimple ω-semigroups, *Proc. Glasgow Math. Assoc.* **7** (1966), 160–169.

UNIVERSITY OF GLASGOW, GLASGOW, W.2

https://doi.org/10.1017/S2040618500035413 Published online by Cambridge University Press