J. Austral. Math. Soc. 20 (Series A) (1975), 172–177.

SEMIGROUPS IN RINGS

J. CRESP* and R. P. SULLIVAN

(Received 16 August 1973)

Communicated by T. E. Hall

1. Introduction

A subset S of a ring R is a left semigroup ideal of R if $RS \subseteq R$, and a left ring ideal of R if in addition S is a subring of R. Gluskin (1960) investigated those rings with 1 which possess the property:

(λ) every left semigroup ideal is a left ring ideal.

Here we study those rings in which every subsemigroup is a subring, and those in which every semigroup endomorphism is a ring endomorphism. We note in passing that recent work on a rather different, but nonetheless related, question: to characterise certain types of semigroups admitting a ring structure, is to be found in Peinado (1970), Satyanarayana (1971) and Satyanarayana (1973).

2. Subsemigroups of Rings

A subset S of R will be called a subsemigroup of R if it is a subsemigroup of $(R, \cdot)$. As usual, for $x \in R$, $\langle x \rangle$ denotes the cyclic subsemigroup of R generated by x. We start by characterising the rings R with the property:

(σ) every subsemigroup of R is a subring.

THEOREM 1. *A ring R has (σ) iff either $|R| = 1$ or $|R| = 2$ and $R^2 = 0$.*

PROOF. Suppose R has (σ) and that $|R| > 1$. Choose $x \in R \backslash 0$ and consider $\langle x \rangle$. Then from (σ), there exists $r \geqq 2$ such that $x^r = 0$: suppose r is the least such integer. Now we also have $x + x^2 = x^t$ for some $t > 0$. If $r > 2$ and $t \geqq 2$, we have $x^{r-2}(x + x^2) = x^{t+r-2}$ and so $x^{r-1} = 0$, contradicting the choice of r. Hence $r > 2$ implies $t = 1$: but then $x^2 = 0$, again contradicting the choice of r. Hence $r = 2$, and we have $x^2 = 0$ for all $x \in R$.

* The work for this paper was begun while a final-year undergraduate student under the supervision of the second author.

In particular, for each $y \in R$, $xy + yx = (x+y)^2 = 0$ and $\{0, x\}$ is a subsemigroup of R for each $x \in R \backslash 0$. Hence from (σ), we have $x + x = 0$ for all $x \in R$ and so $xy + xy = 0$ for all $y \in R$; it follows that R is commutative.

Now suppose $x, y \in R \backslash 0$. Since $\{0, x, xy\}$ is a subsemigroup of R, and R has (σ), we see that $x + xy$ equals 0, xy, or x. In the first case, we obtain $x = xy$ (since $x + x = 0$) and so $0 = xy^2 = xy$ and $x = 0$, a contradiction. If $x + xy = xy$, then $x = 0$ trivially and we again obtain a contradiction. So we must have $x + xy = x$, in which case $xy = 0$. But then $\{0, x, y\}$ is a subsemigroup of R and so from (σ) we deduce that $x + y$ equals x, y or 0. In the first two cases, either x or y will equal 0, a contradiction in either case. Hence, $x + y = 0$ and so $x = y$; that is, $|R \backslash 0| = 1$ and the result follows.

For the converse, suppose $R = \{0, a\}$, $a \neq 0$, and $a^2 = 0$. Then $a + a$ must equal 0, and so the subsemigroups $\{0\}$ and $\{0, a\}$ are seen to be subrings.

In the light of the above proof, we now weaken (σ), and consider those rings R with:

(σ') every subsemigroup containing 0 is a subring.

In order to characterise all such rings containing 1, we shall need two lemmas: the first summarises Theorems 1 and 3 of Gluskin (1960); the proof of the second can be readily deduced from standard results on finite fields (see Burton (1970)).

LEMMA 1. *If R is a ring with* 1 *which satisfies* (λ) *and G denotes the group of units in R, then* $R = G \cup G + 1$.

LEMMA 2. *If F is a finite field and a generator of $F \backslash 0$ has order q where q is odd, then* $|F| = 2^m$ *for some* $m \geqq 1$.

THEOREM 2. *A ring R containing* 1 *has* (σ') *iff it is a finite field such that* $|R \backslash 0|$ *is a prime number.*

PROOF. Since (σ') implies (λ), we deduce from Lemma 1 that $R = G \cup G + 1$ where G is the group of units in R. But $G \cup 0$ is a subsemigroup of R, and so from (σ'), $G \cup 0$ is a subring. In particular, since $1 \in G$, we have $G + 1 \subseteq G \cup 0$ and so $R = G \cup 0$, a division ring.

Now $\{0, 1\}$ is a subsemigroup of R and so (σ') implies that $1 + 1 = 0$. Hence $x + x = 0$ for all $x \in R$. Suppose there exists $x \in R \backslash \{0, 1\}$: we note that if $R = \{0, 1\}$, then it is a field of the required type. Then $S = \langle 1 + x \rangle \cup \{0, 1\}$ is also a subsemigroup of R, and so (σ') implies that $x = 1 + (1 + x) = (1 + x)^t$ for some $t > 1$. But $T = \langle x \rangle \cup \{0, 1\}$ is another subsemigroup of R and so again using (σ') we obtain $1 + x = x^s$ for some $s > 1$. Hence, for each $x \in R \backslash \{0, 1\}$, there exists $r > 1$ such that $x^r = 1$, and so from Jacobson's Theorem (see Burton (1970)) we deduce that R is a field.

If $x \in R \backslash \{0, 1\}$, let q be the least integer such that $x^q = 1$, and suppose

$q = 2k$. Then $\{0, 1, x^k\}$ is a subsemigroup in which, by choice of q, $x^k \neq 1$. But by applying (σ') we obtain a contradiction. Hence q is odd, and $T = \langle x \rangle \cup 0$ is a finite field with a generator having odd order. By Lemma 2, $|T| = 2^m$ for some $m \geqq 1$ and $q = 2^m - 1$; we assert that in addition q is prime.

For, suppose $q = ab$: since q is odd, both a, b are odd. Then $\langle x \rangle$ will contain subgroups $A = \langle x^a \rangle$ and $B = \langle x^b \rangle$ of order b and a respectively, and so by (σ'), $A \cup 0$ and $B \cup 0$ are finite fields, each with a generator having odd order. Therefore by Lemma 2, there exists u, $v \geqq 1$ such that $a = 2^u - 1$, $b = 2^v - 1$. Hence

$$2^m - 1 = q = ab = (2^u - 1)(2^v - 1),$$

and so

$$2^{m-1} - 1 = 2^{u+v-1} - 2^{u-1} - 2^{v-1},$$

a contradiction if both u, $v > 1$. So either $u \leqq 1$ or $v \leqq 1$, and hence either $a = 1$ or $b = 1$.

We have now shown that for each $x \in R\backslash\{0, 1\}$, x has odd prime order. Suppose $x \in R\backslash\{0, 1\}$ and there exists a non-zero $y \in R\backslash\langle x \rangle$. Then $xy \in R\backslash\{0, 1\}$ and if x,y have prime order p, q respectively, then xy has non-prime order pq, a contradiction. Hence $R = \langle x \rangle \cup 0$ is a finite field of order 2^m for which $2^m - 1$ is prime.

Suppose conversely that R is such a field. Then $\langle x \rangle$ is a cyclic group of prime order, and so any element of $\langle x \rangle$ is a generator of $\langle x \rangle$. Hence if S is a subsemigroup of R containing 0 and if there exists $x \in S\backslash\{0, 1\}$, then $S = R$ is certainly a subring; that is, R has (σ'), and the proof is complete.

3. Semigroup endomorphisms

A semigroup endomorphism of a ring R is a mapping $\phi: R \to R$ such that $(xy)\phi = x\phi \cdot y\phi$ for all $x, y \in R$; a ring endomorphism is a semigroup endomorphism $\phi: R \to R$ such that $(x + y)\phi = x\phi + y\phi$ for all $x, y \in R$. We start by considering the following property of a ring R.

(ε) every semigroup endomorphism is a ring endomorphism.

THEOREM 3. *If R is a commutative ring with (ε), then either* (i) $|R| = 1$, *or* (ii) $|R| = 2$ and $R^2 = 0$, *or* (iii) $R = R^2$ *and* $a + a = 0 = a^2$ *for all* $a \in R$.

PROOF. Consider the mapping $\theta_n: R \to R$ defined by setting $x\theta_n = x^n$ for all $x \in R$. Since R is commutative, θ_n is a semigroup endomorphism for each $n \geqq 1$, and hence since R has (ε), each θ_n is a ring endomorphism. Then putting $n = 2$, we obtain $xy + xy = 0$ for all $x, y \in R$, and from $n = 3$, we obtain $xy^2 + x^2y = 0$. But then $x^2 + x^2 = 0$ and so $xy^2 = x^2y$ for all $x, y \in R$. In particular, $x^5 = x^4$ when $y = x^2$, and so x^4 is an idempotent. Now fix $a \in R$ and define $\gamma: R \to R$

by setting $x\gamma = a^4$ for all $x \in R$. Since γ is clearly a semigroup endomorphism, we deduce from (ε) that $a^4 = 0$ for all $a \in R$.

Now suppose $a \in R\backslash 0$ and define $\tau_a\colon R \to R$ and $\mu_a\colon R \to R$ by

$$x\tau_a = \begin{cases} 0 & \text{if } x \in R^2 \\ a^2 & \text{if } x \notin R^2 \end{cases} \qquad x\mu_a = \begin{cases} 0 & \text{if } x \in R^2 \\ a & \text{if } x \notin R^2. \end{cases}$$

If $x, y \in R$, then $xy \in R^2$ and so $(xy)\tau_a = 0$. If either $x \in R^2$ or $y \in R^2$, then $x\tau_a \cdot y\tau_a = 0$, and if both $x, y \notin R^2$, then $x\tau_a \cdot y\tau_a = a^2 \cdot a^2 = 0$. Hence τ_a is a semigroup endomorphism, and so by (ε), is a ring endomorphism. Suppose $v \in R^2$ and $u \notin R^2$. If $v + u \in R^2$, then

$$a^2 = v\tau_a + \mu\tau_a = (v+u)\tau_a = 0.$$

We assert that now μ_a is a semigroup endomorphism. For if $x, y \in R$, then $xy \in R^2$ and $(xy)\mu_a = 0$, and if either $x \in R^2$ or $y \in R^2$, then $x\mu_a \cdot y\mu_a = 0$; if $x, y \notin R^2$, then $x\mu_a \cdot y\mu_a = a \cdot a = 0$. From (ε) we now deduce that

$$a = v\mu_a + u\mu_a = (v+u)\mu_a = 0,$$

a contradiction. Hence if $u \notin R^2$ and $v \in R^2$, then $u + v \notin R^2$.

Now suppose there exists $c \in R\backslash R^2$ and define $\kappa_a\colon R \to R$ and $\lambda_a\colon R \to R$ by

$$x\kappa_a = \begin{cases} 0 & \text{if } x \in R^2 \cup c \\ a^2 & \text{otherwise} \end{cases} \qquad x\lambda_a = \begin{cases} 0 & \text{if } x \in R^2 \cup c \\ a & \text{otherwise.} \end{cases}$$

If $x, y \in R$, then $xy \in R^2 \cup c$, and so $(xy)\kappa_a = 0$. If either $x \in R^2 \cup c$ or $y \in R^2 \cup c$, then $x\kappa_a \cdot y\kappa_a = 0$, and if both $x, y \notin R^2 \cup c$, then $x\kappa_a \cdot y\kappa_a = a^2 \cdot a^2 = 0$. Hence κ_a is a semigroup endomorphism which from (ε) is also a ring endomorphism. Suppose $u, v \in R^2 \cup c$ and $u + v \notin R^2 \cup c$. Then

$$a^2 = (u+v)\kappa_a = u\kappa_a + v\kappa_a = 0,$$

and so as in the case of μ_a above, we can deduce that λ_a is a semigroup endomorphism. But then (ε) implies that $a = (u+v)\lambda_a = u\lambda_a + v\lambda_a = 0$, a contradiction. Hence, if $u, v \in R^2 \cup c$, then $u + v \in R^2 \cup c$. In particular, $xy + c \in R^2 \cup c$ for all $x, y \in R$. But we know from the above that $xy + c \notin R^2$. Hence, $xy + c = c$ and so $R^2 = 0$.

Now define $\delta\colon R \to R$ by setting $0\delta = 0$ and $x\delta = a$ for all $x \in R\backslash 0$. If $x, y \in R$, we know that $xy = 0$ and so $(xy)\delta = 0$. If either $x = 0$ or $y = 0$, then $x\delta \cdot y\delta = 0$, and if $x \neq 0$ and $y \neq 0$, then $x\delta \cdot y\delta = a^2 = 0$. Hence δ is a semigroup endomorphism which is by (ε) a ring endomorphism. So, if there exist $x, y \neq 0$ in R such that $x - y \neq 0$, then $0 = a - a = x\delta - y\delta = (x-y)\delta = a$, a contradiction. Hence, $R = \{0, a\}$ and so (ii) holds.

https://doi.org/10.1017/S1446788700020474 Published online by Cambridge University Press

Suppose now that $R\backslash R^2 = \square$; that is, $R = R^2$. Then for each $a \in R$, $a = xy$ for some $x, y \in R$ and so from an earlier comment, $a + a = 0$. In addition, $a^2 = (xy)^2 = x^2y^2 = (x^2)^2y = 0$, and so (iii) holds.

REMARK. If $|R| = 1$ or if $|R| = 2$ and $R^2 = 0$, then R has (ε): it is not known whether rings satisfying condition (iii) in the above theorem exist, nor whether, if they do, they have (ε).

As in Section 2, we now weaken (ε), and investigate those rings R with: (ε') every non-constant semigroup endomorphism is a ring endomorphism.

THEOREM 4. *If R is a commutative ring with* 1 *and satisfies* (ε'), *then R is a field of order* 2.

PROOF. Let $\theta_n: R \to R$ be defined by setting $x\theta_n = x^n$ for all $x \in R$. Then since R is commutative, θ_n is a semigroup endomorphism of R, and is non-constant since $1\theta_n = 1$ and $0\theta_n = 0$ and $0 \neq 1$. Hence (ε') implies that θ_2 is a ring endomorphism, and so for all $x \in R$, $(x+1)^2 = (x+1)\theta_2 = x^2 + 1$; that is, $x + x = 0$ for all $x \in R$. Likewise θ_3 is a ring endomorphism, and for all $x \in R$

$$(x+1)^3 = (x+1)\theta_3 = x^3 + 1;$$

that is, $x^2 + x = 0$ (since $x + x = 0$) and so $x = x^2$ for all $x \in R$. Hence R is Boolean.

Now let $a \in R\backslash\{0, 1\}$ and define $\gamma: R \to R$ by:

$$\begin{aligned} x\gamma &= a \quad \text{if} \quad xa \neq a \\ &= x \quad \text{if} \quad xa = a \end{aligned}$$

We assert that γ is a non-constant semigroup endomorphism of R. For, suppose $x, y \in R$ and $xya \neq a$. Then $(xy)\gamma = a$ and we may suppose without loss of generality that $xa \neq a$: if $xa = a = ya$, then $xya = a$ since R is Boolean and this is a contradiction. So, $x\gamma \cdot y\gamma = a \cdot y\gamma$ and this equals $a \cdot a$ if $ya \neq a$ or ay if $ya = a$: therefore in either case $x\gamma \cdot y\gamma = a = (xy)\gamma$. If on the other hand $xya = a$, then $xa = x^2ya = xya = a$ and $ya = a$ similarly. Hence in this case also, $(xy)\gamma = xy = x\gamma \cdot y\gamma$. Finally, γ is non-constant since for example $1\gamma = 1$ and $0\gamma = a \neq 1$, and so our assertion holds. But now (ε') implies that γ is a ring endomorphism and so in particular $0\gamma = 0$; that is, $a = 0$, a contradiction. Hence there is no such a in R and we have $|R| = 2$.

In the above theorem, commutativity of R was essentially used to establish the existence of certain semigroup endomorphisms defined on R: it is unknown whether an arbitrary ring, with or without 1, has at least one semigroup endomorphism that can be defined on R in some algebraic manner. The next result replaces the criterion of commutativity by one suggested by Mr. J. S. V. Symons: it holds in, for example, all full matrix rings.

THEOREM 5. *If R is a ring with 1 in which every 1-sided unit is 2-sided and which has* (ε'), *then R is a field of order* 2.

PROOF. Let L be the set of left-units, and G the set of units, in R. Define $\gamma: R \to R$ by:

$$x\gamma = \begin{cases} x & \text{if } x \in G \\ 0 & \text{if } x \notin G. \end{cases}$$

We assert that γ is a non-constant semigroup endomorphism of R. For, if $x, y \in R$ and $xy \in G$, then $(xy)\gamma = xy$ and $x \in L$. Hence $x \in G$ and so $y = x^{-1}xy \in G$. From the definition of γ, we therefore have

$$x\gamma \cdot y\gamma = xy = (xy)\gamma.$$

On the other hand, if $xy \notin G$, then without loss of generality we may assume $x \notin G$. Then

$$(xy)\gamma = 0 = 0 \cdot y\gamma = x\gamma \cdot y\gamma,$$

and clearly $1\gamma = 1$, $0\gamma = 0$, and $1 \neq 0$ imply that γ is non-constant. By (ε'), γ is therefore a ring endomorphism. Now suppose $x \in G$, $y \notin G$. If $x + y \notin G$, we have $x + 0 = x\gamma + y\gamma = (x + y)\gamma = 0$ and $0 \in G$, which is impossible. Hence $x + y \in G$. But then $x + 0 = x\gamma + y\gamma = (x + y)\gamma = x + y$ and so $R \backslash G = \{0\}$; that is, R is a division ring.

Now define $\lambda: R \to R$ by setting $0\lambda = 0$ and $x\lambda = 1$ for all $x \in R \backslash 0$. If $x, y \in R$ and $xy = 0$, then $x = 0$ or $y = 0$, and so $(xy)\gamma = 0 = x\gamma \cdot y\gamma$. If $xy \neq 0$, then both $x, y \neq 0$ and we have $(xy)\gamma = 1 = x\gamma \cdot y\gamma$. Hence γ is a semigroup endomorphism which is obviously non-constant. By (ε'), γ is therefore a ring endomorphism. Now suppose there exists $x \in R \backslash \{0, 1\}$. If $x + x \neq 0$, we have $1 + 1 = x\gamma + x\gamma = (x + x)\gamma = 1$, which is impossible. Hence $x + x = 0$ and so $1 + x \neq 0$. But now $1 + 1 = 1\gamma + x\gamma = (1 + x)\gamma = 1$. Hence $R = \{0, 1\}$ and the result follows.

References

D. M. Burton (1970), *A first course in the theory of rings and ideals* (Addison-Wesley, London, 1970).

L. M. Gluskin (1960), 'Ideals in rings and their multiplicative semigroups', *Uspedni Mat. Nauk.* (*N. S.*) **15**, No. 4 (94), 141–148; translated in *Amer. Math. Soc. Translations*, **27** (2) (1963), 297–304.

R. E. Peinado (1970), 'On semigroups admitting ring structure', *Semigroup Forum* **1**, 189–208.

M. Satyanarayana (1971), 'On semigroups admitting ring structure', *Semigroup Forum* **3**, 43–50,

M. Satyanarayana (1973), 'On semigroups admitting ring structure II', *Semigroup Forum* **6**, 189–197.

University of Western Australia
Nedlands
W.A. 6009
Australia.