J. Austral. Math. Soc. **24** (Series A) (1977), 305–308.

A NOTE ON SEMIGROUPS IN RINGS

STEVE LIGH

(Received 1 November, 1975; revised 20 December 1976)

Communicated by T. E. Hall

1. Introduction

Recently J. Cresp and R. P. Sullivan (1975) investigated those rings R with the following properties:

(*) every multiplicative subsemigroup of R is a subring.

(**) every multiplicative subsemigroup of R containing 0 is a subring.

For rings with (*) they obtained the following characterization.

PROPOSITION 1. *A ring R has (*) if and only if either $|R| = 1$ or $|R| = 2$ and $R^2 = 0$.*

For rings with (**) they characterized all such rings with an identity by employing a result of Gluskin (1963).

PROPOSITION 2. *A ring R containing an identity has (**) if and only if it is a finite field such that $|R - 0|$ is a prime number.*

The purpose of this note is to furnish a characterization of those rings with (**) without assuming an identity and the use of Gluskin's result. Also we will consider some generalizations.

2. Subsemigroups of rings

A subset S of a ring $(R, +, .)$ will be called a subsemigroup of R if it is a subsemigroup of $(R, .)$. As usual, for each x in R, $\langle x \rangle$ denotes the cyclic subsemigroup of R generated by x. In this section we characterize completely those rings with property (**). Our theorem follows from a series of lemmas.

LEMMA 1. *Let R be a ring with (**). If there is $e \neq 0$ in R such that $e^2 = e$, then $x + x = 0$ for all x in R.*

PROOF. Since $\{0, e\}$ is a subsemigroup, it follows that $e + e = 0$. Hence

$ex + ex = (e + e)x = 0$ and $xe + xe = x(e + e) = 0$ for all x in R. Thus $\{0, e\} \cup \langle x + x \rangle$ is a subsemigroup of R, and since R has $(**)$, we see that $e + x + x$ equals 0, e or $(x + x)^j$ for some positive integer j. If $e + x + x = 0$, then $x + x = e$ and $ex + ex = e^2 = 0$, a contradiction. If $e + x + x = (x + x)^j$, then $e = e(e + x + x) = e(x + x)^j = (ex + ex)(x + x)^{j-1} = 0$, a contradiction. Thus the remaining case yields the fact the $e + x + x = e$ and $x + x = e + e = 0$.

LEMMA 2. *Let R be a ring with $(**)$. If there is $e^2 = e \neq 0$ in R, then $ex = xe = x$ for all x in R.*

PROOF. From Lemma 1, $x + x = 0$ for each x in R. Suppose $exe + ex \neq 0$. Also $exe + ex \neq e$. For if not, $exe + ex = e$ implies that $0 = exe + exe = e^2$. Thus $\{0, e\} \cup \langle exe + ex \rangle$ is a subsemigroup and it follows that $exe + ex + e$ equals $0, e$ or $(exe + ex)^j$ for some positive integer j. Now $exe + ex + e = 0$ implies that $exe + ex = e$ and $exe + exe = e^2 = 0$, a contradiction. Similarly, $exe + ex + e = e$ implies that $exe + ex = 0$. Thus we must have that $exe + ex + e = (exe + ex)^j$. Hence $(exe + ex + e)e = (exe + ex)^{j-1}(exe + exe) = 0$. But this means that $exe + exe + e = 0$ and $e = 0$, a contradiction. Hence $exe + ex = 0$ and $exe = ex$. By a similar argument, $exe = xe$ and it follows that $ex = xe$ for each x in R.

Next we wish to establish that $ex = x$ for each x in R. Observe that $ex + x = e$ implies that $ex + ex = e^2 = 0$. Thus $ex + x \neq e$. Suppose $ex + x \neq 0$. Then $\{0, e\} \cup \langle ex + x \rangle$ is a subsemigroup. Again, $ex + x + e$ equals 0, e or $(ex + x)^j$. It can be checked as in the above argument that each of the three possibilities gives a contradiction. Thus we conclude that $ex + x = 0$ and $ex = x$ for each x in R.

LEMMA 3. *Let R be a ring with $(**)$. If there is an x in R such that for all positive integers $n, x^n \neq 0$, then there is an $e^2 = e \neq 0$ in R.*

PROOF. Suppose $x^n \neq 0$ for each positive integer n. Then $x + x = 0$. For if not, since $\{0\} \cup \langle x \rangle$ is a subsemigroup, $-x = x^j$ for some positive integer $j > 1$. Hence $x^2 = (-x)(-x) = x^{2j}$. Thus there is an integer k such that $(x^k)^2 = x^k$. Thus $x^k = e = e^2$. But by Lemma 1, $x + x = 0$, a contradiction.

From above it follows that $x^i + x^i = 0$ for each positive integer i. Again from the subsemigroup $\{0\} \cup \langle x \rangle$, we have that $x + x^2 = x^j, j \geqq 3$ and observe that $(x + x^{j-1})x = x = x(x + x^{j-1})$, or $x + x^2 = 0$ (in which case we let $e = x$). Now we wish to show that $(x + x^{j-1})$ is an idempotent: it follow from the calculation below.

https://doi.org/10.1017/S1446788700020322 Published online by Cambridge University Press

$$(x + x^{j-1})(x + x^{j-1}) = x^2 + x^j + x^j + x^{j-1}x^{j-1}$$
$$= x + x^{j-1}(x + x^{j-1})$$
$$= x + x^{j-1}.$$

Now we are ready to state and prove our main result.

THEOREM 1. *A ring R has property $(**)$ if and only if either $|R| = 1$ or $|R| = 2$ and $R^2 = 0$ or R is a finite field and $|R - 0|$ is a prime number.*

PROOF. Suppose R has $(**)$ and there is an element $x \neq 0$ in R such that $x^n \neq 0$ for each positive integer n. By Lemma 3, there is an $e = e^2 \neq 0$ in R and by Lemma 2, e is the identity of R. By Proposition 2, R is a finite field and $|R - 0|$ is a prime number. Now suppose $|R| > 1$ and every $x \neq 0$ in R is nilpotent. By following the proof of Theorem 1 by Cresp and Sullivan (1975) we see that $|R| = 2$ and $R^2 = 0$.

The converse is immediate and thus the proof of the theorem is complete.

3. Generalizations

In this section we extend Propositions 1 and 2 to the class of near-rings and Gluskin's result (1963) will not be needed in one of the proofs (Theorem 3). For definitions and basic facts about near-rings, see Ligh (1969). Furthermore, replace "subring" by "sub-near-ring" in the definition of property $(*)$ and $(**)$.

THEOREM 2. *A near-ring R has property $(*)$ if and only if either $|R| = 1$ or $|R| = 2$ and $R^2 = 0$.*

PROOF. Using a similar argument to the first part of the proof of Theorem 1 by Cresp and Sullivan (1975), we have that $x^2 = 0$ for each x in R. Thus $0x = (0x)(0x) = 0$ and $\{0, x\}$ is a subsemigroup. It follows that $x + x = 0$ for each x in R and $(R, +)$ is commutative.

Now suppose $x \neq 0$ and $y \neq 0$ are in R. Then $x(x + y)(x + y) = 0$ implies $(x^2 + xy)(x + y) = 0$ and hence $xyx = 0$. Thus $\{0, x, xy\}$ is a subsemigroup and by $(*)$, $x + xy = 0, x$ or xy. A quick calculation shows that $xy = 0$. Similarly $yx = 0$.

Now consider the subsemigroup $\{0, x, y\}$. It follows that $x + y = 0$ and $x = y$. Hence $|R| = 2$ and $R^2 = 0$.

THEOREM 3. *Let R be a near-ring with identity 1. If R has property $(**)$, then R is a near-field. Furthermore, if R is finite, then R is a field such that $|R - 0|$ is a prime number.*

PROOF. Since $\{0,1\}$ is a subsemigroup, $1+1=0$ and hence $(R,+)$ is abelian. Suppose $x \neq 0, 1$ is in R. Then $\{0,1\} \cup \langle x+1 \rangle$ is a subsemigroup of R, and by $(**)$, $x = 1 + (1+x) = (1+x)^j$ for some $j \geqq 2$. On the other hand, $\{0,1\} \cup \langle x \rangle$ is also a subsemigroup, thus $(1+x) = x^s$ for some $s \geqq 2$. Hence there is a positive integer $n \geqq 2$ such that $x^n = x$ and suppose n is the smallest. Again from the subsemigroup $\{0,1\} \cup \langle x \rangle$, we have that $(1 + x^{n-1})$ equals 0, 1 or x^t. Since the second and third possibilities give a contradiction, it follows that $x^{n-1} = 1$ and hence each $x \neq 0$ in R has a multiplicative inverse and R is therefore a near-field.

Suppose the near-field R is finite. Since $1+1=0$ in R, R has characteristic 2 and by Corollary 2 in Ligh, McQuarrie and Slotterbeck (1972), the order of R is 2^n for some positive integer n. Let $2^n - 1 = p_1^{n_1} \cdots p_j^{n_j}$ where each p_i is an odd prime. Since $(R - 0, .)$ is a group, for each $p_i^{n_i}$, there is a subgroup S_i of order $p_i^{n_i}$. Thus the semigroup $0 \cup S_i$ has order $p_i^{n_i} + 1 = 2^{m_i}$. By Theorem 1 in Ligh and Neal (1974), $n_i = 1$ for each i. Hence

$$2^n - 1 = (2^{m_1} - 1)(2^{m_2} - 1) \cdots (2^{m_j} - 1).$$

By expanding the right-hand side of the above equation, one gets a contradiction if $j \geqq 2$. Thus $2^n - 1 = p$ and $(R - 0, .)$ is a commutative group. It follows that R is a field.

References

J. Cresp and R. P. Sullivan (1975), 'Semigroups in rings', *J. Austral. Math. Soc.* **20**, 172–177.

L. M. Gluskin (1963), 'Ideals in rings and their multiplicative semigroups', *Uspedni Mat. Nauk. (N. S.)* **15**, 4 (94), 141–148; translated in *Amer. Math. Soc. Translations*, **27** (2) 297–304.

Steve Ligh (1969), "On boolean near-rings", *Bull. Austral. Math. Soc.* **1**, 375–379.

Steve Ligh, Bruce McQuarrie and Oberta Slotterbeck (1972), 'On near-fields', *J. London Math. Soc.* (2) **5**, 87–90.

Steve Ligh and Larry Neal (1974), 'A note on Mersenne numbers', *Math. Magazine* **47**, 231–233.

Department of Mathematics,
University of Southwestern Louisiana,
Lafayette, Louisiana, USA.