Semigroup Forum (2009) 79: 413–416
DOI 10.1007/s00233-009-9140-6

SHORT NOTE

Ring semigroups whose subsemigroups intersect

Greg Oman

Received: 10 October 2008 / Accepted: 13 January 2009 / Published online: 4 March 2009

Abstract A multiplicative semigroup S is said to be a ring semigroup provided there exists an addition $+$ on S such that $(S, +, \cdot)$ is a ring. In this note, we characterize the ring semigroups S with the property that every two nonzero subsemigroups intersect.

Keywords Ring semigroup · Jacobson's theorem · Nilring · Absolutely algebraic field

As stated above, a multiplicative semigroup S is said to be a *ring semigroup* provided an addition $+$ may be defined on S such that $(S, +, \cdot)$ is a ring. Ring semigroups with special properties have been well-studied in the literature (see [1, 3, 5, 6], and [7], for example).

In this note, we study ring semigroups for which any two nonzero subsemigroups intersect. The main theorem we invoke to prove our result is due to Jacobson [4] which we recall below. The reader might recall that Jacobson's Theorem is a generalization of Wedderbern's famous result that every finite division ring is a field.

Proposition 1 (Jacobson) *Let D be a division ring, and suppose that for all nonzero $x \in D$, there exists a positive integer n (depending on x) such that $x^n = 1$. Then D is commutative.*

Before proceeding, we prove two preliminary lemmas.

Lemma 1 *Let S be a multiplicative semigroup with 0. Then every two nonzero subsemigroups intersect iff for all nonzero $x, y \in S$, there exist positive integers m and n such that $x^m = y^n$.*

Communicated by Benjamin Steinberg.

G. Oman (✉)
Otterbein College, Department of Mathematics, One Otterbein College, Westerville, OH 43081-2006, USA
e-mail: goman@otterbein.edu

Proof Trivial. □

Lemma 2 *Suppose R is a ring without zero divisors. Suppose further that x is a nonzero element of R such that either $xe = x$ or $ex = x$ for some $e \in R$. Then R has an identity.*

Proof Suppose $xe = x$ and $x \neq 0$ (the case $ex = x$ is handled similarly). Then note that also $e \neq 0$. Multiplying on the right by e yields $xe^2 = xe$. Since $x \neq 0$ and R has no zero divisors, $e^2 = e$. Since e is idempotent, it follows that e is the identity of R (see [2], p. 6, Exercise 1(b), for example). □

We now state and prove our main result.

Theorem 1 *Let S be a ring semigroup and let $+$ be an operation such that $(S, +, \cdot)$ is a ring. Then the nonzero subsemigroups of S intersect iff one of the following holds:*

(i) *S is a nilring (i.e. every element of S is nilpotent).*
(ii) *S is an absolutely algebraic field of prime characteristic p.*

Proof If S is a nilring, the result is clear. If (ii) holds, then it is easy to see that every nonzero element of S has finite multiplicative order, and hence by Lemma 1 the nonzero subsemigroups of S intersect.

We now suppose that S is a ring semigroup whose nonzero subsemigroups intersect and consider the ring $(S, +, \cdot)$. If every element of S is nilpotent, then S belongs to family (i) and we are done.

Thus we suppose that S has at least one element x which is not nilpotent. We first claim that 0 is the only nilpotent element of S. Suppose by way of contradiction that there exists a nonzero nilpotent element $y \in S$. Thus $y^k = 0$ for some positive integer k. By Lemma 1, $x^m = y^n$ for some positive integers m and n. But then $x^{mk} = y^{nk} = (y^k)^n = 0^n = 0$. This contradicts the fact that x is not nilpotent, and the claim is established.

We now show that S has no zero divisors. For suppose that $xy = 0$ for some nonzero elements x and y. Again by Lemma 1, there exist positive integers m and n such that $x^m = y^n$. Since $xy = 0$, clearly $x^m y = 0$. As $x^m = y^n$, we obtain $y^{n+1} = 0$. This contradicts the fact that there are no nonzero nilpotent elements.

We arrive at the heart of the proof which is showing that S has a multiplicative identity. Fix an arbitrary nonzero element $\alpha \in S$. We assume first that there exists a prime number p such that $p\alpha = 0$. In this case, note that $p\alpha^n = 0$ for every positive integer n. Suppose now that $\alpha + \alpha^2 = \alpha + \alpha^3 = 0$. Then $\alpha^2 = \alpha^3 = \alpha^2(\alpha)$. It follows from Lemma 2 that S has an identity. Hence we may assume that either $\alpha + \alpha^2 \neq 0$ or $\alpha + \alpha^3 \neq 0$. Let us suppose that $\alpha + \alpha^2 \neq 0$ (the case $\alpha + \alpha^3 \neq 0$ being analogous). By Lemma 1, there exist positive integers m and n such that $(\alpha + \alpha^2)^m = \alpha^n$.

Multiplying out on the left, we obtain

$$\alpha^m + a_{m+1}\alpha^{m+1} + \cdots + a_{2m-1}\alpha^{2m-1} + \alpha^{2m} = \alpha^n \tag{1}$$

for some integers $a_{m+1}, \ldots, a_{2m-1}$. Suppose first that $n < m$. Then we may factor out α^n on the left of (1) to obtain $\alpha^n(\alpha^{m-n} + a_{m+1}\alpha^{m+1-n} + \cdots + a_{2m-1}\alpha^{2m-1-n} + \alpha^{2m-n}) = \alpha^n$. It follows from Lemma 2 that R has an identity. Suppose now that $m < n$. Subtracting, (1) becomes $\alpha^m = \alpha^n - a_{m+1}\alpha^{m+1} - \cdots - a_{2m-1}\alpha^{2m-1} - \alpha^{2m}$. Now factor out α^m on the right to get $\alpha^m = \alpha^m(\alpha^{n-m} - a_{m+1}\alpha - \cdots - a_{2m-1}\alpha^{m-1} - \alpha^m)$. By Lemma 2 again, S has an identity. Lastly, we suppose $m = n$. Cancelling α^m, (1) reduces to

$$a_{m+1}\alpha^{m+1} + \cdots + a_{2m-1}\alpha^{2m-1} + \alpha^{2m} = 0 \tag{2}$$

Recall that α^n has additive order p for every positive integer n. Since $\alpha^{2m} \neq 0$, it follows that not all of the a_i are divisible by p. Without loss of generality, assume a_{m+1} is not divisible by p. Subtracting and factoring, (2) becomes $\alpha^{m+1}(a_{m+2}\alpha + \cdots + \alpha^{m-1}) = -a_{m+1}\alpha^{m+1}$. As a_{m+1} is not divisible by p, $-a_{m+1}$ has an inverse r mod p. Multiplying both sides by r, we have $\alpha^{m+1}(ra_{m+2}\alpha + \cdots + r\alpha^{m-1}) = \alpha^{m+1}$. We are now done as before by Lemma 2. Thus we may now assume that $p\alpha \neq 0$ for any prime number p. Suppose that there exists a prime number p such that $(p\alpha)^n = \alpha^m$ for some natural numbers m and n with $n > m$. Factoring out α^m on the left, we obtain $\alpha^m(p^n\alpha^{n-m}) = \alpha^m$ and we're done as before. Now suppose that there exists a prime number p such that $(p\alpha)^n = \alpha^n$ for some positive integer n. In this case, we obtain $p^n\alpha^n - \alpha^n = 0$. But then $(p^n - 1)\alpha^n = 0$. Since R has no zero divisors, it follows easily that $(p^n - 1)\alpha^i = 0$ for every positive integer i. Write $p^n - 1 = q_1 \cdots q_k$ where each q_i is prime (the case $p = 2$ and $n = 1$ is impossible). Now consider $(q_1\alpha)(q_2\alpha)\cdots(q_k\alpha) = (p^n - 1)\alpha^k = 0$. Since R has no zero divisors, this forces some $q_i\alpha = 0$, contradicting our assumption that $p\alpha \neq 0$ for any prime number p. Thus we finally may assume that for every prime number p, there exist natural numbers m and n such that $(p\alpha)^n = \alpha^m$ and $n < m$. In particular, we have $(2\alpha)^n = \alpha^m$ and $(3\alpha)^j = \alpha^k$ where $n < m$ and $j < k$. Thus $2^n\alpha^n = \alpha^m$ and $3^j\alpha^j = \alpha^k$. Since R has no zero divisors, we obtain $2^n\alpha = \alpha^{m-n+1}$ and $3^j\alpha = \alpha^{k-j+1}$. Let $a, b \in \mathbb{Z}$ be such that $a2^n + b3^j = 1$. We have $a2^n\alpha = a\alpha^{m-n+1}$ and $b3^j\alpha = b\alpha^{k-j+1}$. Adding, we obtain $(a2^n + b3^j)\alpha = a\alpha^{m-n+1} + b\alpha^{k-j+1}$. Since $a2^n + b3^j = 1$, we get $\alpha = a\alpha^{m-n+1} + b\alpha^{k-j+1}$. Since $n < m$ and $j < k$, we may factor out an α on the right, and we are finally done by Lemma 2.

Since S has a 1, it now follows from Lemma 1 that for every nonzero x, there exists a positive integer n such that $x^n = 1$. Now the hypotheses of Jacobson's Theorem are satisfied, and it follows that S is a field. Clearly S must have prime characteristic p since otherwise 2 would have infinite multiplicative order. Since every nonzero $x \in S$ satisfies $x^n = 1$ for some positive integer n, it follows that S is algebraic over $\mathbb{F}_p$. This completes the proof. □

As a corollary, we obtain the following characterization of the finite fields. We leave the proof to the reader.

Corollary 1 *Let R be a ring which contains at least one element which is not nilpotent. Then R is a finite field iff there exists a positive integer k such that $x^k = y^k$ for all nonzero $x, y \in R$.*

References

1. Bell, H.E.: Commutativity in ring semigroups. In: Words, Languages and Combinatorics, II, Kyoto, 1992, pp. 24–31. World Scientific, Singapore (1994)
2. Clifford, A.H., Preston, G.B.: The Algebraic Theory of Semigroups. Mathematical Surveys, no. 7, vol. 1. American Mathematical Society, Providence (1961)
3. Hannah, J., Richardson, J.S., Zeleznikow, J.: Completely semisimple ring semigroups. J. Aust. Math. Soc. Ser. A **30**(2), 150–156 (1980/81)
4. Jacobson, Nathan: Structure theory for algebraic algebras of bounded degree. Ann. Math. **46**, 695–707 (1945)
5. Jones, P.: Rings with a certain condition on subsemigroups. Semigroup Forum **47**(1), 1–6 (1993)
6. Jones, P., Ligh, S.: Quasi ring-semigroups. Semigroup Forum **17**(2), 163–173 (1979)
7. Oman, G.: Ring semigroups whose subsemigroups form a chain. Semigroup Forum (2009) doi:10.1007/s00233-008-9100-6