Semigroup Forum (2009) 78: 374–377
DOI 10.1007/s00233-008-9100-6

SHORT NOTE

Ring semigroups whose subsemigroups form a chain

Greg Oman

Received: 7 January 2008 / Accepted: 6 July 2008 / Published online: 30 July 2008

Abstract A multiplicative semigroup S is called a *ring semigroup* if an addition may be defined on S so that $(S,+,\cdot)$ is a ring. Such semigroups have been well-studied in the literature (see Bell in Words, Languages and Combinatorics, pp. 24–31, World Scientific, Singapore, 1994; Jones in Semigroup Forum 47(1):1–6, 1993; Jones and Ligh in Semigroup Forum 17(2):163–173, 1979). In this note, we use Mihăilescu's Theorem (formerly Catalan's Conjecture) to characterize the ring semigroups whose subsemigroups containing 0 form a chain with respect to set inclusion.

Keywords Ring semigroup · Catalan's conjecture · Quasi-cyclic group · Chain semigroup

For the purposes of this note, let us call a multiplicative semigroup with zero in which the subsemigroups containing zero are linearly ordered under set inclusion a 0-*chain semigroup*. We note that the structure of semigroups whose subsemigroups are linearly ordered by set inclusion (chain semigroups) has been completely determined [7, 8]. We also note that a 0-chain semigroup need not be a chain semigroup. As a trivial example, $\mathbb{Z}/(2)$ (under multiplication) is a 0-chain semigroup but is not chain since $\{0\}$ and $\{1\}$ are incomparable subsemigroups. Lastly, we remark that we consider the chain condition only for subsemigroups containing zero because otherwise the results are trivial (the only nonzero ring in which the multiplicative subsemigroups are linearly ordered is the ring R on two elements where $R^2=0$). We now begin with several lemmas.

Communicated by Michael W. Mislove.

G. Oman (✉)
Department of Mathematics, The Ohio State University, 231 W. 18th Ave., Columbus, OH 43210, USA
e-mail: ggoman@gmail.com

Lemma 1 *Let S be a semigroup with zero. Then S is a 0-chain semigroup iff for any nonzero elements $x, y \in S$, there exists a positive integer n such that either $x = y^n$ or $y = x^n$.*

Proof Suppose first that S is a 0-chain semigroup. Let x, y be arbitrary nonzero elements of S. Let $S_1 := \{0\} \cup \{x^n : n \geq 1\}$ and $S_2 := \{0\} \cup \{y^n : n \geq 1\}$. Since S is a 0-chain semigroup, we may suppose that $S_1 \subseteq S_2$. In particular, $x \in S_2$. Since $x \neq 0$, it follows that $x = y^n$ for some positive integer n. Conversely, suppose for every nonzero x and y there is a positive integer n with $x = y^n$ or $y = x^n$. Suppose by way of contradiction that there exist two subsemigroups S_1 and S_2 of S, both containing 0, but $S_1 \nsubseteq S_2$ and $S_2 \nsubseteq S_1$. Choose $x \in S_1 - S_2$ and $y \in S_2 - S_1$. Note that x and y are nonzero. Thus without loss of generality we may assume that $x = y^n$ for some positive integer n. Since $y \in S_2$, this forces $x \in S_2$, a contradiction. □

Lemma 2 *Suppose that S is a 0-chain semigroup. Let $x \in S$ and suppose that n is the least positive integer such that $x^n = 0$. Then $n \leq 3$.*

Proof Assume S is a 0-chain semigroup. Suppose by way of contradiction that n is least such that $x^n = 0$ and $n \geq 4$. Consider the nonzero elements x^{n-1} and x^{n-2}. We first claim that these two elements are distinct. For suppose that $x^{n-1} = x^{n-2}$. Multiplying through by x yields $x^n = x^{n-1}$. Since $x^n = 0$, also $x^{n-1} = 0$, and this contradicts the minimality of n. By Lemma 1, there exists a positive integer m such that either $x^{n-1} = (x^{n-2})^m = x^{m(n-2)}$ or $x^{n-2} = (x^{n-1})^m = x^{m(n-1)}$. Since $x^{n-1} \neq x^{n-2}$, $m > 1$. But since $n \geq 4$, it follows that $m(n-2) \geq n$. Thus either $x^{n-1} = 0$ or $x^{n-2} = 0$, and this is a contradiction. □

Lemma 3 *Let S be a 0-chain semigroup. Suppose $x \in S$ and $x^3 = 0$ but $x^2 \neq 0$. Then $S = \{0, x, x^2\}$.*

Proof We suppose S is a 0-chain semigroup and $x \in S$ with $x^3 = 0$ but $x^2 \neq 0$. Suppose by way of contradiction that there exists an element $y \notin \{0, x, x^2\}$. Note that y is not equal to a positive power of x since $x^3 = 0$. Hence by Lemma 1, we have $x = y^n$ for some positive integer $n \geq 2$. Squaring both sides yields $x^2 = y^{2n}$. Hence $y^{2n} \neq 0$. Note also that $0 = x^3 = y^{3n}$. Thus a power of y is zero, but $2n \geq 4$ and $y^{2n} \neq 0$. This contradicts Lemma 2. □

Lemma 4 *Let S be a 0-chain semigroup. Suppose $x \in S$ is nonzero and $x^2 = 0$. Then $S = \{0, x\}$ or there exists $y \in S$ with $y^3 = 0$, $y^2 = x$, and $S = \{0, y, y^2\}$.*

Proof Let S be a 0-chain semigroup. Suppose $x \in S$ is nonzero and $x^2 = 0$. If $S = \{0, x\}$, we are done. Thus suppose there is some $y \notin \{0, x\}$. It is clear from Lemma 1 that $x = y^n$ for some positive integer $n > 1$. Recalling that $x^2 = 0$, we obtain $y^{2n} = 0$. Since $y^2 \neq 0$, it follows from Lemmas 2 and 3 that $y^3 = 0$ and $S = \{0, y, y^2\}$. Since $y \neq x$, it follows that $y^2 = x$. This completes the proof. □

We now recall that for a fixed prime p, the direct limit of the cyclic groups $\mathbb{Z}/(p^n)$ is called the quasi-cyclic group of type p^∞ and is commonly denoted by $C(p^\infty)$. We will use the following result of Rosenfeld.

Lemma 5 [7] *Suppose S is an infinite semigroup whose subsemigroups form a chain under set inclusion. Then $S \cong C(p^\infty)$ for some prime p.*

We also recall Catalan's Conjecture. This conjecture was proved in 2002 by Mihăilescu [6] and after his solution, the conjecture now bears his name.

Proposition 1 (Mihăilescu's Theorem) *The only solution to the equation $x^a - y^b = 1$ in the natural numbers for $x, a, y, b > 1$ is $x = 3$, $a = 2$, $y = 2$, $b = 3$.*

This theorem will be of paramount importance in proving our main result. First we prove a final lemma.

Lemma 6 *Let p be a prime number. The quasi-cyclic group $C(p^\infty)$ is not the multiplicative group of nonzero elements of any field.*

Proof Suppose by way of contradiction that $C(p^\infty)$ is the multiplicative group of nonzero elements of some field F. Since $C(p^\infty)$ is a torsion group, it is clear that F has prime characteristic q. It is also clear that since $F^\times \cong C(p^\infty)$, every nonzero $x \in F$ satisfies $x^{p^n} = 1$ for some natural number n. In particular, F is algebraic over its prime subfield $\mathbb{F}_q$. Hence F has subfields of order q^n for arbitrarily large n. Thus we may choose $n > 1$ such that F has $\mathbb{F}_{q^n}$ as a subfield and $q^n - 1 > p^3$. Since $F^\times \cong C(p^\infty)$, it follows that $q^n - 1 = p^m$ for some natural number m. Since $q^n - 1 > p^3$, we must have $m > 3$. Since $n > 1$ and $m > 3$, we have a contradiction to Mihăilescu's Theorem above. This completes the proof. □

We now determine all rings R for which the multiplicative subsemigroups of R containing 0 are linearly ordered.

Theorem 1 *Let R be a ring. Then the multiplicative subsemigroups of R containing 0 are linearly ordered iff one of the following holds*:

(1) $|R| \le 2$
(2) $R \cong \mathbb{F}_q$ *where q is prime and $q = 2^n + 1$ for some $n > 0$*
(3) $R \cong \mathbb{F}_{2^n}$ *where $2^n - 1$ is a (Mersenne) prime*
(4) $R \cong \mathbb{F}_9$.

Proof That the rings in (1)–(4) satisfy the condition is easy to check. Conversely, suppose that R is any ring in which the multiplicative subsemigroups of R containing 0 are linearly ordered. If $|R| \le 2$, then R belongs to family (1) and we're done. Thus we assume $|R| \ge 3$. We now suppose there exists a nonzero x and a positive integer n for which $x^n = 0$. By Lemmas 2, 3, and 4, $R = \{0, y, y^2\}$ for some $y \in R$ with $y^3 = 0$. By Lagrange's Theorem, $y^2 + y^2 \ne 0$. Thus we must have $y^2 + y^2 = y$. Multiplying this equation through by y and using the fact that $y^3 = 0$, we obtain $y^2 = 0$, a contradiction. Hence R has no nonzero nilpotent elements. We claim that this forces R to be a field. Let x and y be arbitrary nonzero elements of R. By Lemma 1, either $x = y^n$ or $y = x^n$ for some positive integer n. This clearly implies that $xy = yx$ and hence R is commutative. Now suppose by way of contradiction that $xy = 0$. Then by Lemma 1, it follows that either $x^k = 0$ or $y^k = 0$ for some positive integer k. This contradicts the established fact that there are no nonzero nilpotent elements. Thus R has no zero divisors. We claim that R is finite. Assume by way of contradiction that R is infinite, and consider the multiplicative semigroup $R - \{0\}$. The subsemigroups of $R - \{0\}$ are linearly ordered, and so it follows from Lemma 5 that $R - \{0\} \cong C(p^\infty)$ for some prime p. This contradicts Lemma 6. Thus R is a finite commutative ring without zero divisors. It is well-known that this implies that R is a field (see [2], Lemma 3.2 on p. 90), whence $R \cong \mathbb{F}_{q^n}$ for some prime q. The subgroups of $\mathbb{F}_{q^n} - \{0\}$ are linearly ordered by inclusion, and it is well-known (see [5], for example) that all such groups are cyclic of prime power order. In particular, this implies that $q^n - 1 = p^m$ for some positive integers n and m. Suppose first that both m a nd n are greater than 1. By Mihăilescu's Theorem, it follows that $q = 3$, $n = 2$, $p = 2$, and $m = 3$. Hence $R \cong \mathbb{F}_9$. Thus we may assume that either $n = 1$ or $m = 1$. Suppose first that $n = 1$. Then $q = p^m + 1$ for some prime p. Clearly p cannot be odd. Thus $q = 2^m + 1$ and R belongs to family (2). Now suppose $m = 1$. Then $q^n - 1 = p$. Clearly q cannot be greater than 3 for then p would be an even prime greater than 2. If $q = 3$, then clearly $n = 1$ and so R belongs to family (2). Otherwise $q = 2$ and R falls into family (3). This completes the proof. □

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. Herstein, I.N.: Topics in Algebra. Blaisdell, Waltham (1964)
3. Jones, P.: Rings with a certain condition on subsemigroups. Semigroup Forum **47**(1), 1–6 (1993)
4. Jones, P., Ligh, S.: Quasi ring-semigroups. Semigroup Forum **17**(2), 163–173 (1979)
5. Lotto, B.: Stacked groups. Am. Math. Mon. **114**(9), 811–812 (2007)
6. Mihăilescu, P.: Primary cyclotomic units and a proof of Catalan's conjecture. J. Reine Angew. Math. **572**, 167–195 (2004)
7. Rosenfeld, A.: Chain semigroups. Port. Math. **32**, 155–156 (1973)
8. Ševrin, L.N.: On lattice properties of semigroups. Sib. Mat. Zh. **3**, 446–470 (1962)