Czechoslovak Mathematical Journal, 59 (134) (2009), 999–1003

THE SEMIRING OF 1-PRESERVING ENDOMORPHISMS OF A SEMILATTICE

JAROSLAV JEŽEK and TOMÁŠ KEPKA, Praha

(Received May 6, 2008)

Abstract. We prove that the semirings of 1-preserving and of 0,1-preserving endomorphisms of a semilattice are always subdirectly irreducible and we investigate under which conditions they are simple. Subsemirings are also investigated in a similar way.

Keywords: semilattice, semiring, subdirectly irreducible, simple

MSC 2010: 06A12, 16Y60

1. INTRODUCTION

Congruence-simple semirings were investigated in the papers [1], [2], [3], [6], [7] and [9]. A special attention was paid to finite, additively idempotent semirings in connection with possible applications to public key cryptography (see [4], [7] and [9]). In the present short paper we investigate for (congruence-) simplicity various endomorphism semirings of semilattices, namely those consisting of endomorphisms preserving the largest and/or the least element.

Let M be a nontrivial (join) semilattice with the largest element that will be denoted by 1_M, or just 1. We denote by $\mathbf{E}_M^1$ the semiring of the endomorphisms f of M such that $f(1) = 1$. If M has also the least element (denoted by 0_M or just 0), we denote by $\mathbf{E}_M^{01}$ the semiring of the endomorphisms f of M such that $f(0) = 0$ and $f(1) = 1$. We will prove that every subsemiring of $\mathbf{E}_M^1$ containing all endomorphisms with range of cardinality at most 2, and also every subsemiring of $\mathbf{E}_M^{01}$ containing all endomorphisms with range of cardinality at most 3, is subdirectly irreducible. The description of their monoliths will make it possible to say precisely which of these

The work is a part of the research project MSM0021620839 financed by MSMT.

subsemirings are simple. The results for $\mathbf{E}^1_M$ and for $\mathbf{E}^{01}_M$ are quite similar. The proofs differ only in details.

2. The interval of semirings between $\mathbf{F}^1_M$ and $\mathbf{E}^1_M$

We denote by $\mathbf{F}^1_M$ the subsemiring of $\mathbf{E}^1_M$ generated by the set Y^1_M of the elements of $\mathbf{E}^1_M$ that are endomorphisms with range of cardinality at most 2. Denote by $\mathbf{G}^1_M$ the subsemiring of $\mathbf{E}^1_M$ consisting precisely of the endomorphisms $f \in \mathbf{E}^1_M$ for which there exists a $g \in Y^1_M$ with $\geqslant g$. It is easy to check that $\mathbf{G}^1_M$ is indeed a semiring and that $\mathbf{F}^1_M \subseteq \mathbf{G}^1_M \subseteq \mathbf{E}^1_M$.

Denote by $\bar{1}$ the largest element of $\mathbf{E}^1_M$, i.e., the constant endomorphism of M with value 1.

For a pair a, b of elements of M such that $b \neq 1$ denote by $\tau_{a,b}$ the endomorphism defined as follows: $\tau_{a,b}(x) = a$ for $x \leqslant b$ and $\tau_{a,b}(x) = 1$ if $x \nleqslant b$. It is easy to see that for M finite, Y^1_M is precisely the set of all the endomorphisms $\tau_{a,b}$ $(a, b \in M,\ b \neq 1)$. This may not be true if M is infinite. For example, let M be the semilattice of nonnegative integers (with respect to the usual ordering of integers) with the largest element added. The endomorphism f sending the largest element to itself and all the other elements to the smallest element belongs to Y^1_M but is not equal to any $\tau_{a,b}$. (It is not even above any $\tau_{a,b}$.)

Theorem 2.1. *Let M be a nontrivial semilattice with* 1. *Every subsemiring E of $\mathbf{E}^1_M$ containing $\mathbf{F}^1_M$ is subdirectly irreducible. Its monolith is the congruence $B^2 \cup \mathbf{id}_E$ where $B = E \cap \mathbf{G}^1_M$.*

Proof. If $f \in B$ then clearly $g \in B$ for any $g \in E$ with $g \geqslant f$. If $f \in B$ and $g \in E$ then $gf \in B$ and $fg \in B$. (Indeed, we have $f \geqslant h$ for some $h \in Y^1_M$; then $gf \geqslant gh$ and $fg \geqslant hg$, where both gh and hg are also at most two-valued.) It follows from these two observations that $B^2 \cup \mathbf{id}_E$ is a congruence of E. Since B has cardinality at least 2, it is a nontrivial congruence.

Let R be an arbitrary nontrivial congruence of E; we need to prove that $B^2 \cup \mathbf{id}_E$ is contained in R. We have $(f, g) \in R$ for two distinct elements f, g of E. Since $f \neq g$, there exists an element $b \in M$ such that either $f(b) \nleqslant g(b)$ or $g(b) \nleqslant f(b)$. Without loss of generality, $g(b) \nleqslant f(b)$. Of course, $b \neq 1$ and $f(b) \neq 1$. For any $a \in M$ we have $(\tau_{a,b}, \bar{1}) = (\tau_{a,f(b)} f \tau_{b,b}, \tau_{a,f(b)} g \tau_{b,b}) \in R$. For any $c \in M$ different from 1 we get $(\tau_{a,c}, \bar{1}) = (\tau_{a,b}\tau_{b,c}, \bar{1}\tau_{b,c}) \in R$. Thus $(\tau_{a,c}, \bar{1}) \in R$ for all $c \neq 1$.

Let $h \in Y^1_M$ and let a be the only element of h in the range of h that is different from 1. From $(\tau_{a,a}, \bar{1}) \in R$ we get $(h, \bar{1}) = (\tau_{a,a} h, \bar{1} h) \in R$.

Since $(h, \bar{1}) \in R$ for all $h \in Y^1_M$, it is clear that also $(h, \bar{1}) \in R$ for all $h \in B$. □

Theorem 2.2. *Let M be a nontrivial semilattice with* 1 *and E a subsemiring of $\mathbf{E}_M^1$ containing $\mathbf{F}_M^1$. Then E is simple if and only if it is contained in $\mathbf{G}_M^1$. In particular, $\mathbf{G}_M^1$ is always simple.*

Proof. This follows immediately from 2.1. □

Theorem 2.3. *Let M be a nontrivial semilattice with* 1*. The semiring $\mathbf{E}_M^1$ is simple if and only if M has the least element and* 1 *is a join-irreducible element of M.*

Consequently, if M is finite then $\mathbf{E}_M^1$ is simple if and only if M is a lattice with a single coatom.

Proof. By 2.2, $\mathbf{E}_M^1$ is simple if and only if $\mathbf{E}_M^1 = \mathbf{G}_M^1$, which takes place if and only if every element of $\mathbf{E}_M^1$ is above at least one element with range of cardinality at most 2.

Let $\mathbf{E}_M^1$ be simple. Then $f \leqslant \mathbf{id}_M$ for some $f \in \mathbf{E}_M^1$ with range contained in $\{a, 1\}$, for some $a \in M$. Put $I = \{x \in M : f(x) = a\}$, so that I is a subsemilattice of M. For all $x \in M$ we have $f(x) \leqslant x$. Thus $a \leqslant x$ for all $x \in I$ and $1 \leqslant x$ for all $x \notin I$. This is possible only if a is the least element of M and $I = M - \{1\}$. Thus $M - \{1\}$ is a subsemilattice, which means that 1 is a join-irreducible element.

Conversely, let M have the least element a and let $M - \{1\}$ be a subsemilattice. Denote by h the endomorphism sending 1 to 1 and any other element of M to a. Then h has the range of cardinality 2 and $f \geqslant h$ for all $f \in \mathbf{E}_M^1$. □

3. The interval of semirings between $\mathbf{F}_M^{01}$ and $\mathbf{E}_M^{01}$

Let M be a nontrivial semiring with the least element 0 and the largest element 1. We denote by $\mathbf{F}_M^{01}$ the subsemiring of $\mathbf{E}_M^{01}$ generated by the set Y_M^{01} of the elements of $\mathbf{E}_M^{01}$ that are endomorphisms with range of cardinality at most 3. Denote by $\mathbf{G}_M^{01}$ the subsemiring of $\mathbf{E}_M^{01}$ consisting precisely of the endomorphisms $f \in \mathbf{E}_M^{01}$ for which there exists a $g \in Y_M^{01}$ with $f \geqslant g$. It is easy to check that $\mathbf{G}_M^{01}$ is indeed a semiring and that $\mathbf{F}_M^{01} \subseteq \mathbf{G}_M^{01} \subseteq \mathbf{E}_M^{01}$.

By an ideal of M we mean a nonempty subset I such that $a, b \in I$ implies $a \vee b \in I$ and $a \in I$ implies $x \in I$ for all $x \leqslant a$. Every ideal of M contains the element 0. An ideal is proper if and only if it does not contain the element 1. For $a \in M$ denote by $\downarrow a$ the ideal $\{x \in M : x \leqslant a\}$.

Let $a \in M$ and let I be a proper ideal of M. We denote by $\eta_{a,I}$ the endomorphism of M defined as follows: $\eta_{a,I}(0) = 0$; $\eta_{a,I}(x) = a$ for $x \in I - \{0\}$; $\eta_{a,I}(x) = 1$ for $x \notin I$. Clearly, $\eta_{a,I} \in \mathbf{E}_M^{01}$.

Put $\bar{1}_0 = \eta_{0,\{0\}}$, so that $\bar{1}_0$ is the largest element of $\mathbf{E}_M^{01}$.

Theorem 3.1. *Let M be a nontrivial semilattice with 0 and 1. Every subsemiring E of $\mathbf{E}_M^{01}$ containing $\mathbf{F}_M^{01}$ is subdirectly irreducible. Its monolith is the congruence $B^2 \cup \mathbf{id}_E$ where $B = E \cap \mathbf{G}_M^{01}$.*

P r o o f. Clearly, $B^2 \cup \mathbf{id}_E$ is a nontrivial congruence of E. Let R be an arbitrary nontrivial congruence of E; we need to prove that $B^2 \cup \mathbf{id}_E$ is contained in R.

Since R is nontrivial, there exists a pair $(f,g) \in R$ such that $f < g$. There is an element $a \in M$ with $f(a) < g(a)$. Put $J = \downarrow f(a)$, so that J is a proper ideal of M. For any proper ideal I we have $(\eta_{0,I}, \bar{1}_0) = (\eta_{0,J}\,;\ f\,;\ \eta_{a,I},\,;\ \eta_{0,J}\,;\ g\,;\ \eta_{a,I}) \in R$.

Let $h \in E$ be an endomorphism with range $\{0,a,1\}$ where $0 \leqslant a < 1$. Put $I = h^{-1}\{0,a\} = \{x \in M : h(x) \in \{0,a\}\}$, so that I is a proper ideal of M. Clearly, $h \geqslant \eta_{0,I}$. Since $(\eta_{0,I}, \bar{1}_0) \in R$, it follows that $(h, \bar{1}_0) \in R$.

Thus $(h, \bar{1}_0) \in R$ for all $h \in Y_M^{01}$. From this it follows that $(h, \bar{1}_0) \in R$ for all $h \in B$. Thus $B^2 \cup \mathbf{id}_E \subseteq R$. □

Theorem 3.2. *Let M be a nontrivial semilattice with 0 and 1 and E a subsemiring of $\mathbf{E}_M^{01}$ containing $\mathbf{F}_M^{01}$. Then E is simple if and only if it is contained in $\mathbf{G}_M^{01}$. In particular, $\mathbf{G}_M^{01}$ is always simple.*

P r o o f. This follows immediately from 3.1. □

Theorem 3.3. *Let M be a nontrivial semilattice with 0 and 1. The semiring $\mathbf{E}_M^{01}$ is simple if and only if 1 is a join-irreducible element.*

Consequently, if M is finite then $\mathbf{E}_M^{01}$ is simple if and only if M is a lattice with a single coatom.

P r o o f. By 3.2, $\mathbf{E}_M^{01}$ is simple if and only if $\mathbf{E}_M^{01} = \mathbf{G}_M^{01}$ if and only if every element of $\mathbf{E}_M^{01}$ is above at least one element with range of cardinality at most 3.

Let $\mathbf{E}_M^{01}$ be simple. Then $f \leqslant \mathbf{id}_M$ for some $f \in \mathbf{E}_M^{01}$ with range contained in $\{0,a,1\}$, for some $a \in M$. Put $I = \{x \in M : f(x) \in \{0,a\}\}$, so that I is a proper ideal of M. For all $x \in M$ we have $f(x) \leqslant x$. Thus $1 \leqslant x$ for all $x \notin I$. This is possible only if $I = M - \{1\}$. Thus $M - \{1\}$ is an ideal of M.

Conversely, let 1 be join-irreducible, so that $M - \{1\}$ is an ideal of M. Then the mapping h, sending 1 to 1 and any other element of M to 0, is an endomorphism of M preserving both 0 and 1. This h has the range of cardinality 2 and $f \geqslant h$ for all $f \in \mathbf{E}_M^{01}$. □

Acknowledgement. We are grateful to Klára Kepková for helping us by managing the run of the LATIAXIS3 program, which has been designed for checking subdirect irreducibility of subsemirings of the full endomorphism semiring of a monoid.

References

[1] *R. El Bashir, J. Hurt, A. Jančařík and T. Kepka*: Simple commutative semirings. J. Algebra *236* (2001), 277–306.
[2] *R. El Bashir and T. Kepka*: Congruence-simple semirings. Semigroup Forum *75* (2007), 588–608.
[3] *J. Ježek, T. Kepka and M. Maróti*: The endomorphism semiring of a semilattice. Semigroup Forum *78* (2009), 253–261.
[4] *G. Maze, C. Monico and J. Rosenthal*: Public Key Cryptography based on semigroup actions. Adv. Math. Commun. *1* (2007), 489–502.
[5] *R. McKenzie, G. McNulty and W. Taylor,*: Algebras, Lattices, Varieties, Volume I. Wadsworth & Brooks/Cole, Monterey, CA, 1987.
[6] *S. S. Mitchell and P. B. Fenoglio*: Congruence-free commutative semirings. Semigroup Forum *37* (1988), 79–91.
[7] *C. Monico*: On finite congruence-simple semirings. J. Algebra *271* (2004), 846–854.
[8] *H. S. Vandiver*: Note on a simple type of algebras in which the cancellation law of addition does not hold. Bull. Amer. Math. Soc. *40* (1934), 916–920.
[9] *J. Zumbrägel*: Classification of finite congruence-simple semirings with zero. Preprint.

Authors' addresses: J. Ježek, Charles University in Prague, Faculty of Mathematics and Physics, Mathematical Institute, Sokolovská 83, 186 75 Prague 8, Czech Republic, jezek@karlin.mff.cuni.cz; T. Kepka, Charles University in Prague, Faculty of Mathematics and Physics, Mathematical Institute, Sokolovská 83, 186 75 Prague 8, Czech Republic, kepka@karlin.mff.cuni.cz.