Open access • Journal Article • DOI:10.1142/S0219498808002862

Classification of finite congruence-simple semirings with zero — Source link

Jens Zumbrägel

Institutions: University of Zurich

Published on: 01 Jun 2008 - Journal of Algebra and Its Applications (World Scientific Publishing Company)

Topics: Semiring, Kleene algebra, Ring (mathematics), Endomorphism and Idempotence

Year: 2008

Classification of finite congruence-simple semirings with zero

Zumbraegel, J

Classification of finite congruence-simple semirings with zero [1]

Jens Zumbrägel

Institut für Mathematik, Universität Zürich
Winterthurerstrasse 190, 8057 Zürich, Switzerland

Abstract

Our main result states that a finite semiring of order > 2 with zero which is not a ring is congruence-simple if and only if it is isomorphic to a 'dense' subsemiring of the endomorphism semiring of a finite idempotent commutative monoid.

We also investigate those subsemirings further, addressing e.g. the question of isomorphy.

Key words: Semirings, Lattices, Endomorphism semirings, Semimodules

1 Introduction and main result

Semirings, introduced by Vandiver [Van34] in 1934, generalize the notion of noncommutative rings in the sense that negative elements do not have to exist. Since then there has been an active area of research in semirings, both on the theoretical side and on the side of applications e.g. in theoretical computer science. The reader may consult the monographs of Golan [Gol99] and Hebisch/Weinert [HW93] for a more elaborate introduction to semirings.

In order to develop a structure theory for semirings, special interest lies in semirings which are congruence-simple, meaning simple in the sense that there are only trivial quotient semirings (see below for precise definitions). The classification of simple commutative semirings was achieved only recently in [BHJK01]. In the general case it has been shown later [Mon04] that any

Email address: jzumbr@math.unizh.ch (Jens Zumbrägel).
[1] This work has been supported by the Swiss National Science Foundation under grant no. 107887.

finite simple semiring of order > 2 which is not a ring has to have either trivial or idempotent addition. In this paper we give a full classification of finite simple semirings assuming they have a zero element.

Definition 1.1. A set R with two binary operations $+$ and $\cdot$ is called a *semiring* (with zero) if $(R, +)$ is a commutative monoid, $(R, \cdot)$ is a semigroup, and the distributive laws $x \cdot (y+z) = x \cdot y + x \cdot z$ and $(x+y) \cdot z = x \cdot z + y \cdot z$ hold for all $x, y, z \in R$; furthermore, the neutral element 0 of $(R, +)$ has to satisfy $0 \cdot x = x \cdot 0 = 0$ for all $x \in R$, and is called *zero*.

We sometimes write the multiplication as concatenation, i.e. $xy := x \cdot y$ for $x, y \in R$. If $(R, \cdot)$ has a neutral element $1 \in R$ we call it *one*. By a *subsemiring* of a semiring R we mean a subset $S \subseteq R$ with $0 \in S$ which is closed under addition and multiplication. Naturally, S itself is a semiring.

As mentioned above our notion of simplicity relies on congruences.

Definition 1.2. An equivalence relation $\sim$ on a semiring R is called *congruence* if

$$x \sim y \quad \text{implies} \quad a + x \sim a + y,\ ax \sim ay,\ xa \sim ya, \quad \text{for all } x, y, a \in R.$$

The semiring R is called *congruence-simple* if its only congruences are $\sim\, = \mathrm{id}_R$ and $\sim\, = R \times R$.

Remark 1.3. Given a congruence $\sim$ on a semiring R, we can define operations $+$ and $\cdot$ on its set of equivalence classes $R/\!\sim\, = \{[x] \mid x \in R\}$ by $[x] + [y] := [x + y]$ and $[x] \cdot [y] := [xy]$, for $x, y \in R$, turning $(R/\!\sim, +, \cdot)$ into a semiring, called the *quotient semiring*.

Note that if R is a ring, there is a one-to-one correspondence between congruences and ideals by identifying a congruence with its 0-class. Hence a ring is congruence-simple if and only if it is simple in the sense that there are only trivial ideals.

By a semiring homomorphism we mean a map $f : R \to S$ between semirings R and S which preserves the semiring operations and the zero element. Note that any homomorphism $f : R \to S$ gives rise to a congruence $\sim$ on R by defining $x \sim y$ if and only if $f(x) = f(y)$, for $x, y \in R$. On the other hand, for any congruence $\sim$ on R we have the natural homomorphism $R \to R/\!\sim$. This easily proves the following

Remark 1.4. A semiring R is congruence-simple if and only if any nonzero homomorphism $f : R \to S$ into a semiring S is injective.

The following example of a semiring turns out to be important.

Example 1.5. Let $(M, +)$ be a commutative monoid. We call a map $f : M \to M$ an endomorphism if it preserves the monoid operation and the neutral element. On the set $\mathrm{End}(M)$ of all endomorphisms of M we get operations $+$ and $\circ$ by defining $f + g$ as pointwise addition and and $f \circ g$ as composition of maps, for $f, g \in \mathrm{End}(M)$.

It is straight-forward to verify that $(\mathrm{End}(M), +, \circ)$ is a semiring with a one, which will be called *endomorphism semiring*.

The classification result uses subsemirings of some endomorphism semirings, which are rich or lie dense in the sense that they contain at least certain elementary endomorphisms.

Definition 1.6. Let M be an idempotent commutative monoid. A subsemiring $S \subseteq \mathrm{End}(M)$ is called *dense* if it contains for all $a, b \in M$ the endomorphism $e_{a,b} \in \mathrm{End}(M)$, defined by

$$e_{a,b}(x) := \begin{cases} 0 & \text{if } x + a = a \\ b & \text{otherwise} \end{cases} \qquad (x \in M).$$

Now we can state the main result.

Theorem 1.7. *Let R be a finite semiring which is not a ring. Then the following are equivalent:*

(1) *R is congruence-simple.*
(2) *$|R| \leq 2$ or R is isomorphic to a dense subsemiring $S \subseteq \mathrm{End}(M)$, where $(M, +)$ is a finite idempotent commutative monoid.*

Note that the classification of finite simple rings is a classical subject in algebra. By the Wedderburn–Artin Theorem (see [Her68]), a finite ring R with nontrivial multiplication is simple if and only if R is isomorphic to the endomorphism ring $\mathrm{Mat}_{n\times n}(\mathbb{F})$ of a finite-dimensional vector space $\mathbb{F}^n$ over a finite field $\mathbb{F}$.

Remark 1.8. There are two proper semirings of order 2, namely the semirings $R_{2,a}$, $R_{2,b}$ given by

$R_{2,a}$:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	0

$R_{2,b}$:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

.

$R_{2,b}$ is called the *Boolean semiring* and can also be seen as the endomorphism semiring $\mathrm{End}(L_2)$ for $(L_2, +) = (\{0,1\}, \max)$. Trivially, $R_{2,a}$ and $R_{2,b}$ are congruence-simple.

The proof of the main result is given in Sections 2 and 3 of this paper. In Section 2 we show the direction (2) ⇒ (1), whereas in Section 3 we establish the direction (1) ⇒ (2) with the help of irreducible semimodules. Finally, we take a closer look at the dense subsemirings of the endomorphism semirings in Section 4.

2 Endomorphism semirings

In this section we shall prove the direction (2) ⇒ (1) of Theorem 1.7. We begin with a remark on idempotent commutative monoids and (semi-)lattices (see e.g. [Bir67, sec. I.5 and II.2]).

Remark 2.1. Let $(M, +)$ be an idempotent commutative monoid. By defining $x \le y$ if and only if $x + y = y$ for $x, y \in M$, we get a partial order relation $\le$ on M, where $0 \le x$ for any $x \in M$. Also, for all $x, y \in M$ there exists a supremum $x \vee y = x + y$, so that $(M, \vee)$ is a join-semilattice.

If in addition M is finite, for all $x, y \in M$ there exists an infimum $x \wedge y = \sum_{z \le x,\, z \le y} z$, so that $(M, \vee, \wedge)$ is even a lattice.

Now if M is viewed as a lattice, the elements $f \in \mathrm{End}(M)$ are maps $f : M \to M$ satisfying $f(0) = 0$ and $f(x \vee y) = f(x) \vee f(y)$ for all $x, y \in M$. In particular, f is order-preserving. Note however that $f(x \wedge y) = f(x) \wedge f(y)$ is not generally true, i.e. f may not be a lattice endomorphism.

Now we state a lemma on the maps $e_{a,b}$ of Definition 1.6. Note that by Remark 2.1 we have

$$e_{a,b}(x) = \begin{cases} 0 & \text{if } x \le a \\ b & \text{otherwise} \end{cases} \qquad (a, b, x \in M).$$

Lemma 2.2. *For $a, b \in M$, we have $e_{a,b} \in \mathrm{End}(M)$. Also, for $f \in \mathrm{End}(M)$ and $a, b, c, d \in M$, we have $f \circ e_{a,b} = e_{a,f(b)}$ and*

$$e_{c,d} \circ f \circ e_{a,b} = \begin{cases} 0 & \textit{if } f(b) \le c, \\ e_{a,d} & \textit{otherwise.} \end{cases}$$

If $(M, +)$ has an absorbing element $\infty \in M$, then $e_{0,\infty}$ is absorbing for $(\mathrm{End}(M), +)$.

Proof. Note that for all $x, y \in M$, we have $x \vee y \leq a$ if and only if $x \leq a$ and $y \leq a$. It follows that $e_{a,b}(x \vee y) = 0$ if and only if $e_{a,b}(x) = 0$ and $e_{a,b}(y) = 0$, that is if and only if $e_{a,b}(x) \vee e_{a,b}(y) = 0$. Thus $e_{a,b} \in \mathrm{End}(M)$.

Now if $f \in \mathrm{End}(M)$ and $a, b \in M$ one easily verifies $f \circ e_{a,b} = e_{a,f(b)}$. Applying this formula twice yields

$$e_{c,d} \circ f \circ e_{a,b} = e_{c,d} \circ e_{a,f(b)} = e_{a,e_{c,d}(f(b))} = \begin{cases} 0 & \text{if } f(b) \leq c, \\ e_{a,d} & \text{otherwise.} \end{cases}$$

Finally, for any $h \in \mathrm{End}(M)$ and $x \in M \setminus \{0\}$ we have $(h + e_{0,\infty})(x) = h(x) + \infty = \infty$, so that $h + e_{0,\infty} = e_{0,\infty}$. ☐

Proposition 2.3. *Let $(M, +)$ be an idempotent commutative monoid with an absorbing element. Then any dense subsemiring $R \subseteq \mathrm{End}(M)$ is congruence-simple. In particular, $\mathrm{End}(M)$ itself is congruence-simple.*

Note that any *finite* idempotent commutative monoid M has an absorbing element, namely $\infty := \sum_{x \in M} x$.

Proof. Let $\sim \subseteq R \times R$ be a semiring congruence relation. Suppose that $\sim \neq \mathrm{id}_R$, so that there exists $f, g \in R$ with $f \neq g$, but $f \sim g$. There is $b \in M$ with $f(b) \neq g(b)$, and without loss of generality, we may assume $f(b) \not\leq c := g(b)$.

For all $a, d \in M$ we have $e_{a,b} \in R$ and $e_{c,d} \in R$. Hence, since $\sim$ is a congruence,

$$e_{c,d} \circ f \circ e_{a,b} \sim e_{c,d} \circ g \circ e_{a,b},$$

so that $e_{a,d} \sim 0$, by Lemma 2.2.

In particular $e_{0,\infty} \sim 0$, where $\infty \in M$ is the absorbing element. It follows that

$$e_{0,\infty} = h + e_{0,\infty} \sim h + 0 = h$$

for any $h \in R$, since $\sim$ is a congruence. Therefore $\sim = R \times R$, so that R has no nontrivial congruence relations. ☐

3 Finite congruence-simple semirings

In this section we prove that any finite congruence-simple semiring which is not a ring is of the form described in Theorem 1.7. We start with a result established and proven by Monico in a more general setting [Mon04] and give a simplified proof for our case.

Proposition 3.1. *Let R be a congruence-simple semiring which is not a ring. Then the addition $(R,+)$ is idempotent.*

Proof. For $x \in R$ and $n \in \mathbb{N}_0 := \{0,1,2,3,\dots\}$ let us write $nx := x + \cdots + x$, summing x n-times. Also let $R + x := \{y + x \mid y \in R\}$. Now, for $x, y \in R$ define

$$x \sim y \quad :\Leftrightarrow \quad \exists\, m, n \in \mathbb{N}_0 : \; mx \in R + y, \; ny \in R + x.$$

Then it is easily verified that $\sim$ is a congruence relation.

By congruence-simplicity it follows that $\sim\, = \mathrm{id}_R$ or $\sim\, = R \times R$. In the first case, since $x \sim x + x$, we deduce that $(R,+)$ is idempotent. In the second case, for all $x \in R$, we have $x \sim 0$, so that $0 \in R + x$. This shows that $(R,+)$ is a group and thus R is a ring. $\square$

Remark 3.2. A congruence-simple semiring R with idempotent addition and trivial multiplication $R\,R = \{0\}$ has order ≤ 2. Indeed, since $(R,+)$ is idempotent, $x + y = 0$ implies $x = y = 0$ for $x, y \in R$, so the equivalence relation $\sim$ on R with classes $\{0\}$ and $R \setminus \{0\}$ is a congruence. Thus $\sim\, = \mathrm{id}_R$ and hence $|R| \leq 2$.

3.1 Semimodules

The concept of semimodules over semirings is well-known (see [Gol99]). For the proof of the classification result, we show that any finite congruence-simple semiring admits a semimodule which is irreducible in a strong sense and then we derive consequences from it.

To fix some notations, let R be a semiring.

Definition 3.3. A (left) *semimodule* M over R is a commutative monoid $(M,+)$ with neutral element $0 \in M$, together with an R-multiplication $R \times M \to M$, $(r,x) \mapsto r \cdot x = rx$, such that, for all $r, s \in R$ and $x, y \in M$, we have $r(sx) = (rs)x,\; 0x = 0,\; r0 = 0,\;$ and $\;(r+s)x = rx + sx,\; r(x+y) = rx + ry$.

Remark 3.4. If $(M,+)$ is a commutative monoid, any representation i.e. semiring homomorphism

$$T : R \to \mathrm{End}(M), \quad r \mapsto T_r$$

turns M into a semimodule by defining $rx := T_r(x)$, for $x \in R$ and $x \in M$.

On the other hand, let M be any semimodule over R. For $r \in R$, the map $x \mapsto rx$ defines an endomorphism T_r of M, and the map $T : R \to \mathrm{End}(M)$, $r \mapsto T_r$ is a representation.

Definition 3.5. Let M be a semimodule over R. A *subsemimodule* $N \subseteq M$ is a submonoid of $(M, +)$ such that $R \cdot N \subseteq N$. An equivalence relation $\sim$ on M is called *congruence* if

$$x \sim y \quad \text{implies} \quad a + x \sim a + y,\ rx \sim ry, \quad \text{for all } x, y, a \in M \text{ and } r \in R.$$

Remark 3.6. Note that any subsemimodule $N \subseteq M$ itself is a semimodule over R. Also, given a congruence $\sim$ on M, we can define an addition and an R-multiplication on its set of equivalence classes $M/{\sim} = \{[x] \mid x \in M\}$ by

$$[x] + [y] := [x + y],\ r[x] := [rx], \quad \text{for all } x, y \in M,\ r \in R,$$

turning $M/{\sim}$ into a semimodule over R, called the *quotient semimodule*.

If M is a semimodule over R, let us call the subsemimodules $\{0\}$ and M and also the quotient semimodules $M/\operatorname{id}_M \cong M$ and $M/(M \times M) \cong \{0\}$ the trivial ones.

Definition 3.7. A semimodule M over R satisfying $R\,M \neq \{0\}$ is called

- *sub-irreducible* if it has only trivial subsemimodules,
- *quotient-irreducible* if it has only trivial quotient semimodules,
- *irreducible* if it is both sub-irreducible and quotient-irreducible.

Some authors refer to sub-irreducible and quotient-irreducible semimodules as minimal and simple semimodules, respectively.

By a semimodule homomorphism we mean a map $f : M \to N$ between semimodules over R which preserves the semimodule operations as well as the zero element. In this case, $f(M)$ is a subsemimodule of N, and the relation $x \sim y$ if and only if $f(x) = f(y)$, for $x, y \in M$, is a congruence on M. On the other hand, for any subsemimodule $N_0 \subseteq N$ and any quotient semimodule $M/{\sim}$ there are natural homomorphisms $i : N_0 \to N$ and $p : M \to M/{\sim}$. This constitutes the following

Remark 3.8. Let M be a semimodule over R such that $R\,M \neq \{0\}$. Then

- M is sub-irreducible if and only if any nonzero homomorphism $f : N \to M$ from a semimodule N is surjective,
- M is quotient-irreducible if and only if any nonzero homomorphism $f : M \to N$ into a semimodule N is injective.

Remark 3.9. To illustrate the use of irreducible semimodules we give a version of Schur's Lemma (see [Her68]): Let M be an irreducible semimodule over R with representation $T : R \to \operatorname{End}(M)$, $r \mapsto T_r$. Then the commuting semiring

$$C(M) := \{f \in \mathrm{End}(M) \mid f \circ T_r = T_r \circ f \text{ for all } r \in R\}$$

is a semifield, i.e. any nonzero element is invertible. Indeed, if $f \in C(M) \setminus \{0\}$, then $f : M \to M$ is a nonzero semimodule homomorphism, which by Remark 3.8 must be injective and surjective. It then easily follows that the inverse f^{-1} lies in $C(M)$.

In particular, if $(M, +)$ is finite and idempotent, then $C(M)$ is a finite proper semifield. It follows (see [HW93, sec. I.5]) that $C(M)$ has order ≤ 2, so that $C(M) = \{0, \mathrm{id}_M\}$ is trivial. If the representation $R \to \mathrm{End}(M)$ is faithful i.e. injective (this holds for example if R is congruence-simple and $R\,M \neq \{0\}$), it follows that R has trivial center, since

$$\{x \in R \mid xr = rx \text{ for all } r \in R\} = T^{-1}(C(M)) = \{0, 1\} \cap R.$$

3.2 Existence of irreducible semimodules

Proposition 3.10. *Any finite congruence-simple semiring R with $R\,R \neq \{0\}$ admits a finite irreducible semimodule.*

To prove this result we begin with two lemmas that guarantee the property $R\,M \neq \{0\}$ for certain semimodules M over R. By a nontotal semimodule congruence on M we mean a congruence $\sim\, \neq M \times M$, so that $M/\!\sim\, \neq \{0\}$.

Lemma 3.11. *Let R be a congruence-simple semiring with $R\,R \neq \{0\}$, considered as a semimodule over itself, and let $\sim$ be a nontotal semimodule congruence on R. Then, for the quotient semimodule $M := R/\!\sim$ we have $R\,M \neq \{0\}$.*

Proof. Since $\sim$ is a semimodule congruence, $r \sim s$ implies $x + r \sim x + s$ and $xr \sim xs$, for any $r, s, x \in R$. Now suppose $R\,M = \{0\}$. Then for any $r, x \in R$ we have $[rx] = r[x] = 0$, so that $rx \sim 0$. Hence $r \sim s$ implies also $rx \sim sx$, for any $r, s, x \in R$, so that $\sim$ is even a semiring congruence. Since $\sim$ is nontotal, we must have $\sim\, = \mathrm{id}_R$ by congruence-simplicity. Hence $M = R$ and $R\,R = \{0\}$, which contradicts our assumption. □

Lemma 3.12. *Let M be a semimodule over R such that $R\,M \neq \{0\}$.*

(1) *If M is sub-irreducible, then $R\,P \neq \{0\}$ for all its nonzero quotient semimodules $P = M/\!\sim$.*
(2) *If M is quotient-irreducible, then $R\,N \neq \{0\}$ for all its nonzero subsemimodules $N \subseteq M$.*

Proof. (1) Let M have only trivial subsemimodules. Since $RM \subseteq M$ is a subsemimodule, we must have $RM = M$. Now let $P = M/\sim$ be a quotient subsemimodule with $RP = \{0\}$. Then we have $M = RM \subseteq [0]_\sim$, and therefore $M/\sim = \{0\}$.

(2) Let $A := \{x \in M \mid Rx = \{0\}\} \subseteq M$ be the annulator of R in M. Then it is easy to check that A is a semimodule of M with the additional property that $x \in A$ and $x + y \in A$ implies $y \in A$. Also it is straightforward to check that defining

$$x \sim y \quad :\Leftrightarrow \quad \exists\, a, b \in A : x + a = y + b$$

for $x, y \in M$ gives a congruence $\sim$ on M such that its zero-class $\{x \in M \mid x \sim 0\}$ equals A. Finally note that $A \neq M$ by assumption.

Now if M has only trivial quotient semimodules, the relation $\sim$ above must equal id_M, and hence $A = \{0\}$. It follows that any subsemimodule $N \subseteq M$ with $RN = 0$ must be zero. □

Proof of Proposition 3.10. We recursively define a sequence $M_0, M_1, \ldots, M_n$ of finite semimodules over R of decreasing sizes such that

- for all $i = 0, \ldots, n$ we have $RM_i \neq \{0\}$,
- for all $i = 1, \ldots, n$ we have M_i is sub-irreducible or quotient-irreducible,
- M_n is irreducible.

We start with $M_0 := R$, so that $RM_0 = RR \neq \{0\}$.

Now let $\sim$ be a maximal nontotal semimodule congruence on R (probably $\sim\, = \mathrm{id}_R$) and let $M_1 := R/\sim$. Since $\sim$ is nontotal we have $RM_1 \neq \{0\}$ by Lemma 3.11. By maximality of $\sim$ it follows that M_1 is quotient-irreducible.

Suppose that M_i has been defined for some $i \geq 1$, so that $RM_i \neq \{0\}$ and M_i is sub-irreducible or quotient-irreducible. If M_i is even irreducible we set $n = i$ and stop.

Otherwise suppose that M_i is quotient-irreducible but has nontrivial subsemimodules. Take a minimal nonzero semimodule $M_{i+1} \subseteq M_i$. Then $RM_{i+1} \neq \{0\}$ by Lemma 3.12, (2), and furthermore M_{i+1} is sub-irreducible. Now consider the case where M_i is sub-irreducible but has nontrivial congruences. By taking a maximal nontotal congruence $\sim$ and letting $M_{i+1} := M_i/\sim$, we have $RM_{i+1} \neq \{0\}$ by Lemma 3.12, (1), and furthermore M_{i+1} is quotient-irreducible.

The sequence has been constructed. Since R is finite and the cardinalities of $M_1, M_2, \ldots$ are strictly decreasing the sequence must terminate by an irreducible semimodule M_n over R. □

Let R be a congruence-simple semiring and M be a semimodule over R with $RM \neq \{0\}$. Then the representation $R \to \mathrm{End}(M)$ is nonzero and hence must be injective, so that R can be seen as a subsemiring of $\mathrm{End}(M)$. If M is irreducible the question of the 'density' of R in $\mathrm{End}(M)$ arises. We have already seen in Remark 3.9 that the commuting semiring of R in $\mathrm{End}(M)$ is trivial if $(M, +)$ is idempotent. Now we show another density result:

Proposition 3.13. *Let R be a finite congruence-simple semiring with idempotent addition and let M be a finite irreducible semimodule over R. Then $(M, +)$ is idempotent, and for all $a, b \in M$ there exists $r \in R$ such that*

$$rx = \begin{cases} 0 & \text{if } x + a = a \\ b & \text{otherwise} \end{cases} \qquad (x \in M).$$

Thus R, seen as a subsemiring of $\mathrm{End}(M)$*, is dense (see Definition 1.6).*

Proof. First note that $(M, +)$ is idempotent: By irreducibility, the subsemimodule RM of M is nonzero, hence $RM = M$. So, any $x \in M$ can be written as $x = ry$ with $r \in R$ and $y \in M$. It follows $x+x = ry+ry = (r+r)y = ry = x$, since $(R, +)$ is idempotent, so that $(M, +)$ is idempotent. Recall from Remark 2.1 that now on M there is an order relation $\leq$ defined by $x \leq y$ if and only if $x + y = y$, for $x, y \in M$.

For $x \in M$ define $I_x := \{r \in R \mid rx = 0\}$, which is a subsemimodule of R. We have $I_{x+y} = I_x \cap I_y$ for $x, y \in M$, since $rx + ry = 0$ implies $rx = ry = 0$ for $r \in R$, because $(M, +)$ is idempotent. Now we claim that defining

$$x \sim y \quad :\Leftrightarrow \quad I_x = I_y \qquad (x, y \in M)$$

gives a semimodule congruence on M: Indeed, if $x \sim y$ and $z \in M$, we have $I_{z+x} = I_z \cap I_x = I_z \cap I_y = I_{z+y}$, so that $z + x \sim z + y$. Also for $r, s \in R$ we have $r(sx) = (rs)x = 0$ if and only if $(rs)y = r(sy) = 0$, so that $I_{sx} = I_{sy}$ i.e. $sx \sim sy$.

Assume that $\sim = M \times M$. Then $I_x = I_0 = R$ for all $x \in M$, so that $RM = \{0\}$, which cannot hold. Since M is quotient-irreducible it follows that $\sim = \mathrm{id}_M$. We conclude that $x \leq y$ is equivalent to $I_y \subseteq I_x$, for $x, y \in M$, since $x + y = y$ if and only if $I_x \cap I_y = I_{x+y} = I_y$.

Now let $a \in M$ be fixed. If $a = \infty$, the absorbing element in $(M, +)$, the assertion trivially holds with $r = 0$. So assume $a \neq \infty$. For any $x \in M$ with $x \not\leq a$ we have shown before that $I_a \not\subseteq I_x$, so the semimodule homomorphism $I_a \to M$, $r \mapsto rx$ is nonzero. Since M is sub-irreducible, it must be surjective, so in particular there exists $r_x \in I_a$ such that $r_x\, x = \infty$. Letting $s := \sum_{x \not\leq a} r_x \in I_a \subseteq R$, for $x \in M$ we have

$$sx = \begin{cases} 0 & \text{if } x \leq a, \ \text{since then } sx = sx + sa = sa = 0, \\ \infty & \text{if } x \not\leq a, \ \text{since then } sx \geq r_x\, x = \infty, \end{cases}$$

so we have shown the assertion for $b = \infty$.

Consider now the subsemimodule $N := \{r\infty \mid r \in R\}$ of M. We have $\infty = s\infty \in N$, so that $N \neq \{0\}$. By sub-irreducibility of M it follows $N = M$, so for any $b \in M$ there exists $r \in R$ with $r\infty = b$. Then for $x \in M$ we have $(rs)x = 0$ if $x \leq a$, and $(rs)x = b$ otherwise, which completes the proof. □

Now we complete the proof of the Theorem 1.7 by showing the direction (1) ⇒ (2). Let R be a finite congruence-simple semiring which is not a ring and suppose $|R| > 2$. Then $(R, +)$ is idempotent by Proposition 3.1 and $R\,R \neq \{0\}$ by Remark 3.2. Afterwards, Proposition 3.10 guarantees the existence of a finite irreducible semimodule M over R, so that R is isomorphic to a subsemiring S of $\mathrm{End}(M)$. Finally, by Proposition 3.13 we have that S is a dense subsemiring of $\mathrm{End}(M)$.

4 The family of dense endomorphism subsemirings

Definition 4.1. Let M be an idempotent commutative monoid. We define $\mathcal{SR}(M)$ to be the collection of all dense subsemirings $R \subseteq \mathrm{End}(M)$.

In this section we take a closer look at the families $\mathcal{SR}(M)$. First we address the question of isomorphy and anti-isomorphy of these semirings. Then we give a criterion when the family $\mathcal{SR}(M)$ is trivial. Finally we list the dense endomorphism subsemirings having smallest order.

In this section, let M, M_1 and M_2 be always idempotent commutative monoids having an absorbing element.

4.1 Isomorphy

Proposition 4.2. *Let $R_1 \in \mathcal{SR}(M_1)$ and $R_2 \in \mathcal{SR}(M_2)$ be isomorphic semirings. Then also the monoids M_1 and M_2 are isomorphic.*

We prove a lemma first. Recall from Lemma 2.2 that if $\infty \in M$ is the absorbing element, then $e_{0,\infty}$ is an absorbing element in $(R, +)$ for any semiring $R \in \mathcal{SR}(M)$.

Lemma 4.3. *Let $R \in \mathcal{SR}(M)$ and let $z \in R$ be the absorbing element in $(R, +)$. Then the map*

$$\vartheta : M \to Rz, \quad b \mapsto e_{0,b}$$

defines an isomorphism between $(M, +)$ and the submonoid Rz of $(R, +)$.

Proof. Note that $f \circ e_{0,\infty} = e_{0,f(\infty)}$ for all $f \in R$, so in particular $e_{0,b} \circ e_{0,\infty} = e_{0,b}$ for all $b \in M$. This shows $Rz = Re_{0,\infty} = \{e_{0,b} \mid b \in M\}$, so ϑ is well-defined and surjective. That ϑ is injective and a homomorphism is clear. □

Proof of Proposition 4.2 Suppose there is a semiring isomorphism $\varphi : R_1 \to R_2$. For $i = 1, 2$, let $z_i \in R_i$ be the absorbing element in $(R_i, +)$. We then have $\varphi(z_1) = z_2$ and thus $\varphi(R_1 z_1) = R_2 z_2$. The restriction $\varphi' = \varphi|_{R_1 z_1} : R_1 z_1 \to R_2 z_2$ of φ is therefore an isomorphism between the submonoids $R_1 z_1$ and $R_2 z_2$ of $(R_1, +)$ and $(R_2, +)$, respectively. Now for $i = 1, 2$, let $\vartheta_i : M_i \to R_i z_i$ be the isomorphism defined in Lemma 4.3. Then we can construct an isomorphism

$$\vartheta_2^{-1} \circ \varphi' \circ \vartheta_1 : M_1 \to M_2$$

between the monoids $(M_1, +)$ and $(M_2, +)$.

Next we identify anti-isomorphic pairs of congruence-simple semirings.

Remark 4.4. Let M be finite with corresponding lattice $(M, \vee, \wedge)$, so that $(M, +) = (M, \vee)$. Then also $(M, \wedge)$ is a finite idempotent commutative monoid, which we denote by $\tilde{M}$. Its corresponding lattice is the *dual lattice* of M, obtained by reversing the order $(M, \leq)$.

Let $(L_2, \vee) = (\{0, 1\}, \max)$ and let $M^* = \operatorname{Hom}(M, L_2)$ be the set of all monoid homomorphisms $M \to L_2$. Defining addition pointwise, M^* becomes a finite idempotent commutative monoid.

Lemma 4.5. *The monoid M^* is isomorphic to $\tilde{M}$. In fact, the map*

$$M \to M^*, \quad a \mapsto e_a, \text{ where } e_a(x) = \begin{cases} 0 & \text{if } x \leq a, \\ 1 & \text{otherwise,} \end{cases}$$

is a bijection such that $e_{a \wedge b} = e_a \vee e_b$ for all $a, b \in M$.

Proof. This is rephrasing the well-known result in lattice theory that any finite lattice is isomorphic to its lattice of ideals (see [Bir67, sec. II.3]). □

Proposition 4.6. *Let M be finite. The semirings $\operatorname{End}(M)$ and $\operatorname{End}(\tilde{M})$ are anti-isomorphic.*

Proof. By Lemma 4.5 we may assume $\tilde{M} = M^*$. Define a map

$$\mathrm{End}(M) \to \mathrm{End}(M^*), \quad f \mapsto f^*, \text{ where } f^*(\varphi) := \varphi \circ f \text{ for } \varphi \in M^*.$$

It is easy to see that this map is well-defined and that the following algebraic properties hold for $f, g \in \mathrm{End}(M)$:

$$(f+g)^* = f^* + g^*, \quad 0^* = 0, \quad (f \circ g)^* = g^* \circ f^*.$$

To prove injectivity, suppose we have $f, g \in \mathrm{End}(M)$ with $f^* = g^*$. With e_a as defined in Lemma 4.5 it follows $e_a(f(x)) = e_a(g(x))$ for all $a, x \in M$, so that $f(x) \leq a$ if and only if $g(x) \leq a$. For all $x \in M$ it follows $f(x) = g(x)$, hence $f = g$.

From injectivity it follows in particular $|\mathrm{End}(M)| \leq |\mathrm{End}(\tilde{M})|$. We can apply this result to $\tilde{M}$ to yield $|\mathrm{End}(\tilde{M})| \leq |\mathrm{End}(M)|$. Thus $|\mathrm{End}(M)| = |\mathrm{End}(\tilde{M})|$ and the map is also surjective. □

Corollary 4.7. *Let M be finite and suppose M as a lattice is isomorphic to its dual lattice. Then the semiring* $\mathrm{End}(M)$ *is anti-isomorphic to itself.*

Corollary 4.8. *Let M_1 and M_2 be finite and let $R_1 \in \mathcal{SR}(M_1)$ and $R_2 \in \mathcal{SR}(M_2)$ be anti-isomorphic semirings. Then the monoids M_1 and $\tilde{M}_2$ are isomorphic.*

Proof. By Proposition 4.6, $\mathrm{End}(M_2)$ is anti-isomorphic to $\mathrm{End}(\tilde{M}_2)$, and thus R_1 is isomorphic to some $R_2' \in \mathcal{SR}(\tilde{M}_2)$. Now the result follows from Proposition 4.2. □

4.2 The case $|\mathcal{SR}(M)| = 1$

We now discuss under which circumstances the only dense subsemiring of $\mathrm{End}(M)$ is $\mathrm{End}(M)$ itself.

Proposition 4.9. *Let M be finite. Then we have $\mathcal{SR}(M) = \{\mathrm{End}(M)\}$ if and only if the lattice $(M, \vee, \wedge)$ satisfies the following condition:*

$$\forall z \in M: \ z = \bigvee_{a,\, z \not\leq a} \ \bigwedge_{x,\, x \not\leq a} x. \tag{D}$$

Proof. If S is the subsemiring of $R := \mathrm{End}(M)$ generated by the set $E := \{e_{a,b} \mid a, b \in M\}$, then we have $\mathcal{SR}(M) = \{\mathrm{End}(M)\}$ if and only if $S = R$. Note that since E is closed under multiplication (see Lemma 2.2) S consists of all finite sums of elements in E. Writing $1 = \mathrm{id}_M \in R$ we show that

$$S = R \quad \text{if and only if} \quad 1 = \sum_{(a,b)\in X} e_{a,b} \text{ with } X := \{(a,b) \in M^2 \mid e_{a,b} \le 1\}. \tag{$*$}$$

Indeed, suppose $S = R$, so we can express in particular 1 as a sum of elements in E, say $1 = \sum_i e_{a_i,b_i}$. Surely, $e_{a_i,b_i} \le 1$ and hence $(a_i, b_i) \in X$ for all i, so that

$$1 = \sum_i e_{a_i,b_i} \le \sum_{(a,b)\in X} e_{a,b} \le 1$$

and thus the right side of $(*)$ holds. On the other hand, supposing $1 = \sum_{(a,b)\in X} e_{a,b}$ implies $1 \in S$. Then for any $f \in R$ we have

$$f = f \circ 1 = \sum_{(a,b)\in X} f \circ e_{a,b} = \sum_{(a,b)\in X} e_{a,f(b)} \in S$$

(see Lemma 2.2), so that $S = R$. This proves the equivalence $(*)$.

Note next that $(a, b) \in X$ i.e. $e_{a,b} \le 1$ if and only if $b \le x$ for all $x \not\le a$ which is equivalent to $b \le \bigwedge_{x,\, x\not\le a} x$. This shows that

$$\sum_{(a,b)\in X} e_{a,b} = \sum_{a\in M} e_{a,b_a} \text{ with } b_a := \bigwedge_{x,\, x\not\le a} x.$$

Now for all $z \in M$ we have

$$\sum_{(a,b)\in X} e_{a,b}(z) = \sum_{a\in M} e_{a,b_a}(z) = \bigvee_{a,\, z\not\le a} b_a = \bigvee_{a,\, z\not\le a} \bigwedge_{x,\, x\not\le a} x,$$

which together with $(*)$ concludes the proof. ☐

Remark 4.10. The condition (D) given in proposition 4.9 is fulfilled if and only if the lattice M is distributive, or equivalently, M is isomorphic to a ring of subsets (cf. [Bir67, sec. III.3]).

Indeed, assume that $(M, \cup, \cap)$ is a ring of subsets, i.e. a sublattice of a power set lattice $(\mathcal{P}(\Omega), \cup, \cap)$. For $\omega \in \Omega$ let $A_\omega := \bigcup_{X\in M, \omega\notin X} X \in M$. Then for $X \in M$ we have $X \subseteq A_\omega$ if and only if $\omega \notin X$. It follows

$$Z \supseteq \bigcup_{A,\, Z\not\subseteq A} \; \bigcap_{X,\, X\not\subseteq A} X \supseteq \bigcup_{\omega,\, Z\not\subseteq A_\omega} \; \bigcap_{X,\, X\not\subseteq A_\omega} X = \bigcup_{\omega,\, \omega\in Z} \; \bigcap_{X,\, \omega\in X} X \supseteq Z$$

for all $Z \in M$, so M satisfies property (D).

On the other hand, if we have a lattice $(M, \vee, \wedge)$ with condition (D), let $\Omega := \{b_a \mid a \in M\}$ with $b_a := \bigwedge_{x,\, x\not\le a} x$. Consider the representation of M

given by

$$\Phi : M \to \mathcal{P}(\Omega), \quad z \mapsto \{b_a \mid a \in M,\, z \not\leq a\}.$$

We can see directly that $z_1 \leq z_2$ implies $\Phi(z_1) \subseteq \Phi(z_2)$. On the other hand, with the help of (D) we conclude that $\Phi(z_1) \subseteq \Phi(z_2)$ implies $z_1 = \bigvee_{a,\, z_1 \not\leq a} b_a \leq \bigvee_{a,\, z_2 \not\leq a} b_a = z_2$. It follows that Φ is a lattice monomorphism, so that M is isomorphic to a sublattice of $(\mathcal{P}(\Omega), \cup, \cap)$.

4.3 Congruence-simple semirings of small order

Table 1 shows the smallest nontrivial idempotent commutative monoids M (up to isomorphy), represented by the Hasse-diagram of the corresponding lattices, together with the semirings in the collection $\mathcal{SR}(M)$. We write R_m for a semiring with m elements.

These, together with $R_{2,a}$ from Remark 1.8, are the smallest congruence-simple semirings which are not rings. The smallest such semiring not shown in Table 1 has order 98.

Note that $R_{50,a}$ and $R_{50,b}$ are anti-isomorphic to each other by Proposition 4.6, whereas the other semirings in Table 1 are self-anti-isomorphic by Corollary 4.7. Furthermore, all semirings in Table 1 have a one-element, except R_{42} and R_{44}.

Acknowledgements

I am very grateful to my advisor Joachim Rosenthal and also to Gérard Maze for their great encouragement and some fruitful discussions.

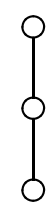
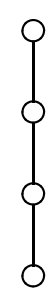
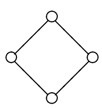
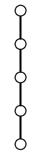
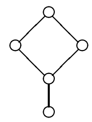
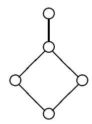
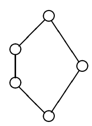
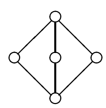
References

[BHJK01] R. El Bashir, J. Hurt, A. Jančařík, and T. Kepka, *Simple commutative semirings*, J. Algebra **236** (2001), 277–306.

[Bir67] G. Birkhoff, *Lattice theory*, 3rd ed., American Mathematical Society, Providence, R.I., 1967.

[Gol99] J. Golan, *Semirings and their applications*, Kluwer Academic Publishers, Dordrecht, 1999.

Table 1
The smallest lattices together with the corresponding endomorphism semirings.

M	$\mathcal{SR}(M)$
	$\{R_{2,b}\}$ (the Boolean semiring)
	$\{R_6\}$
	$\{R_{20}\}$
	$\{R_{16}\}$ (the 2×2-matrices over R_2)
	$\{R_{70}\}$
	$\{R_{50,a}\}$
	$\{R_{50,b}\}$
	$\{R_{43},\ R_{42}\}$
	$\{R_{50,c}, R_{47}, R_{46,a}, R_{46,b}, R_{46,c}, R_{45}, R_{44}\}$ (where $R_{46,a}$, $R_{46,b}$ and $R_{46,c}$ are isomorphic)

[Her68] I. N. Herstein, *Noncommutative rings*, Mathematical Association of America, Washington, D.C., 1968.

[HW93] U. Hebisch and H. J. Weinert, *Halbringe. Algebraische Theorie und Anwendungen in der Informatik.*, B. G. Teubner, Stuttgart, 1993.

[Mon04] C. Monico, *On finite congruence-simple semirings*, J. Algebra **271** (2004), no. 2, 846–854, arXiv:math.RA/0205083.

[Van34] H. S. Vandiver, *Note on a simple type of algebra in which the cancellation law of addition does not hold*, Bull. Am. Math. Soc. **40** (1934), 914–920.