A CONSTRUCTION OF CONGRUENCE-SIMPLE SEMIRINGS

Barbora Batíková
Department of Mathematics
CULS, Kamýcká 129
165 21 Praha 6-Suchdol
Czech Republic
batikova@tf.czu.cz

Tomáš Kepka
Department of Algebra
MFF UK, Sokolovská 83
186 75 Praha 8
Czech Republic
kepka@karlin.mff.cuni.cz

Petr Němec*
Department of Mathematics
CULS, Kamýcká 129
165 21 Praha 6-Suchdol
Czech Republic
nemec@tf.czu.cz

Abstract. A construction of congruence-simple semirings is presented.

The congruence-simple semirings of positive rational (real) numbers are fairly familiar, but the other (congruence-)simple semirings are regarded as somewhat apocryphal. It is easy to show that simple semirings split into three basic classes: the additively cancellative semirings, the additively nil-semirings and the additively idempotent ones. The first class includes all simple rings and many subsemirings of ordered rings. The second class includes many congruence-simple semigroups equipped with constant addition, but what remains is quite enigmatic so far ([1]). Now, we come to the third class, the additively idempotent simple semirings. These semirings (at least in the finite case) are of interest because of possible applications in cryptology (see e.g. [9]) and they are constructed as endomorphism semirings of semilattices (see [2], [6], [7] and [8]). The present note continues this line of research. Finally, notice that few pieces of information on simple semirings and general semirings are available in [4] or [5].

∗. Corresponding author

1. Preliminaries

Let $A = A(*)$ be a groupoid. An element $a \in A$ is called *left (right) neutral* if $a * x = x$ ($x * a = x$) for all $x \in A$, and *left (right) absorbing* if $a * x = a$ ($x * a = a$) for all $x \in A$. If $A = A(+)$ then $0_A \in A$ ($o_A \in A$) means that 0_A (o_A) is (the unique) left and right neutral (absorbing) element of $A(+)$ and $0_A \notin A$ ($o_A \notin A$) denotes the fact that $A(+)$ has no (left and right) neutral (absorbing) element. Similarly, if $A = A(\cdot)$ then $1_A \in A$ means that 1_A is (the unique) left and right neutral element of $A(\cdot)$.

A semilattice is a commutative and idempotent semigroup. If M ($= M(+)$) is a semilattice then a basic order $\leq$ is defined on M by $x \leq y$ iff $x + y = y$. Now, an element $w \in M$ is the smallest (greatest, resp.) element of the ordered set $M(\leq)$ if and only if $w = 0_M$ ($w = o_M$, resp.).

A non-empty subset I of M is an *ideal* if $M + I = I$. This ideal is said to be *prime* if $M \setminus I$ is a subsemilattice of M. For every $x \in N = M \setminus \{o_M\}$ (here and throughout the paper $N = M$ if $o_M \notin M$ and similarly for $M \setminus \{0_M\}$), the set $A_x = \{\, y \in M \mid y \not\leq x \,\}$ is called *principal prime ideal determined by the element* x. Clearly, a subset I of M is a prime ideal if and only if the set $V = M \setminus I$ is a proper subsemilattice of M such that $x \in V$ whenever $x \leq y \in V$. This prime ideal is principal if and only if $o_V \in V$.

A *semiring* is a non-empty set equipped with two associative binary operations that are usually written as addition and multiplication. The addition is commutative and the multiplication distributes over the addition. Given a semiring S, a *(left S-)semimodule* (${}_SM =$) M is a commutative semigroup $M(+)$ together with a scalar multiplication $S \times M \to M$ such that $(a+b)x = ax + bx$, $a(x + y) = ax + ay$ and $a(bx) = (ab)x$ for all $a, b \in S$ and $x, y \in M$. If S is a semiring then $R = \underline{R}(S) = \{\, a \in S \mid Sa = \{a\} \,\}$ denotes the set of right multiplicatively absorbing elements. If $a \in \underline{R}(S)$ then $a + a = aa + aa = (a + a)a = a$ and $a(b + b) = ab + ab = ab$ for every $b \in S$. Consequently, the semiring S is additively idempotent, provided that the right semimodule $\underline{R}(S)_S$ is faithful, i.e., for all $a, b \in S$, $a \neq b$, there is at least one $x \in \underline{R}(S)$ with $xa \neq xb$.

Let S be a semiring. A non-empty subset I of S is a *left (right) ideal* of S if $SI \cup (I + I) \subseteq I$ ($IS \cup (I + I) \subseteq I$). A left (right) ideal I is called *minimal* if $|I| \geq 2$ and $J = I$ whenever J is a left (right) ideal with $|J| \geq 2$ and $J \subseteq I$. A non-empty subset I of S is an *ideal* if $SI \cup IS \cup (I + I) \subseteq I$ and it is a *bi-ideal* if $SI \cup IS \cup (I + S) \subseteq I$. In the latter case, the relation $(I \times I) \cup \mathrm{id}_S$ is a congruence of the semiring S. Finally, S is called

– *simple* (more precisely: *congruence–simple*) if S has just two congruence relations (then these are id_S and $S \times S$ and $|S| \geq 2$);
– *(bi–)ideal–simple* if $S = I$ whenever I is an (bi–)ideal of S with $|I| \geq 2$.

Throughout the paper, all semirings and semimodules are assumed to be additively idempotent. It means that the respective additive semigroups $M(+)$ are semilattices.

2. Auxiliary results (a)

Throughout this section, let S be an (additively idempotent) semiring such that $|R| \geq 2$.

2.1 Lemma. (i) *If $0_S \in S$ then $0_R \in R$, $R0_S = \{0_R\}$ and $S0_S \leq 0_R$.*
(ii) *If $o_S \in S$ then $o_R \in R$, $Ro_S = \{o_R\}$ and $o_R \leq So_S$.*

Proof. $a0_S+b = a0_S+ab = a(0_S+b) = ab$ and $ao_S+b = ao_S+ab = a(o_S+b) = ao_S$ for all $a \in S$ and $b \in R$. □

2.2 Lemma. *Assume that either $R + S = S$ or the right semimodule R_S is faithful. Then:*
(i) *If $0_S \in S$ then $0_S = 0_R \in R$.*
(ii) *If $0_R \in R$ then $0_R = 0_S \in S$.*

Proof. (i) By 2.1(i), $ab0_S = 0_R = a0_S$ for all $a \in R$ and $b \in S$, and hence $b0_S = 0_S$, provided that R_S is faithful. If $R+S = S$ then $0_R+S = 0_R+R+S = R + S = S$.
(ii) $a(b + 0_R) = ab + a0_R = ab + 0_R = ab$ for all $a \in R$ and $b \in S$. □

2.3 Lemma. *Assume that either $R \cap (S + a) \neq \emptyset$ for every $a \in S$ or the right semimodule R_S is faithful. Then:*
(i) *If $o_S \in S$ then $o_S = o_R \in R$.*
(ii) *If $o_R \in R$ then $o_R = o_S \in S$.*

Proof. Using 2.1(ii), we proceed similarly as in the proof of 2.2. □

2.4 Lemma. *If the semiring S is simple then the right semimodule R_S is faithful.*

Proof. Take into account that $ab = b \neq c = ac$ for all $a \in S$ and $b, c \in R$, $b \neq c$. □

2.5 Lemma. (i) *R is the smallest (right) ideal of S.*
(ii) *$R + S$ is the smallest bi-ideal of R.*

Proof. It is easy. □

2.6 Corollary. (i) *The semiring S is ideal-simple iff $R = S$.*
(ii) *The semiring S is bi-ideal-simple iff $R + S = S$.* □

2.7 Lemma. *If the semiring S is simple then $R + S = S$ and the right semimodule R_S is faithful and simple.*

Proof. By 2.4 and 2.6(ii), R_S is faithful and $R+S=S$. If α is a congruence of R_S then ϱ is a congruence of S, where $(a,b)\in\varrho$ iff $(ca,cb)\in\alpha$ for every $c\in R$. Of course, $\varrho\cap(R\times R)=\alpha$. □

2.8 Lemma. *Let the right semimodule R_S be faithful and simple. If $\varrho\neq\mathrm{id}_S$ is a congruence of the semiring S then $R\times R\subseteq\varrho$.*

Proof. Let $(a,b)\in\varrho$, $a,b\in S$, $a\neq b$. Since R_S is faithful, $ca\neq cb$ for at least one $c\in R$, so that $\alpha=\varrho\cap(R\times R)\neq\mathrm{id}_R$. Clearly, α is a congruence of R_S, and therefore $\alpha=R\times R$. □

2.9 Lemma. *Assume that $R+S=S$. The following conditions are equivalent:*

(i) *$\varrho=S\times S$, whenever ϱ is a congruence of S such that $R\times R\subseteq\varrho$.*

(ii) *For every $a\in S$ there is $b\in R$ with $a\leq b$.*

Proof. (i) implies (ii). Define a relation σ on S by $(a,b)\in\sigma$ iff $(a+R)\cap(b+R)\neq\emptyset$. Then σ is a congruence of S and $R\times R\subseteq\sigma$. Thus $\sigma=S\times S$.
(ii) implies (i). If $a,b\in S$ then $a\leq c$, $b\leq d$ and $e\leq a$, $f\leq b$ for some $c,d,e,f\in R$. Now, $(a,c)=(a+e,a+c)\in\varrho$, $(b,d)=(b+f,b+d)\in\varrho$, $(c,d)\in\varrho$ and, finally, $(a,b)\in\varrho$. □

2.10 Proposition. *The semiring S is simple iff the right semimodule R_S is both faithful and simple and the ideal R is both upwards and downwards cofinal in S.*

Proof. The direct implication follows from 2.4, 2.7 and 2.9, while the converse one from 2.8 and 2.9. □

2.11 Lemma. *Assume that $ac=bc$ for all $a,b\in R$, $c\in S$ and put $\mu(c)=ac$. Then μ is a homomorphism of the semiring S onto the semiring R and $\mu|R=\mathrm{id}_R$. Further, the left semimodule ${}_SR$ is not faithful, and if the right semimodule R_S is faithful then $S=R$ and $\mu=\mathrm{id}_R$.*

Proof. Easy to check. □

2.12 Lemma. (i) *If the right semimodule R_S is faithful and $S\neq R$ then $ac\neq bc$ for some $a,b\in R$ and $c\in S$.*
(ii) *If the left semimodule ${}_RS$ is faithful then for all $a,b\in R$, $a\neq b$, there is $c\in S$ with $ac\neq bc$.*
(iii) *If the right semimodule R_S is simple and the left semimodule ${}_RS$ is not faithful then $ac=bc$ for all $a,b\in R$ and $c\in S$.*

Proof. Use 2.11. □

3. Auxiliary results (b)

Let S be a non-trivial semiring. A (left S-)semimodule M ($=_S M$) will be called characteristic if the following conditions are satisfied:

(a) $|M| \geq 3$;

(b) $0_M \in M$ and $S0_M = \{0_M\}$;

(c) $o_M \in M$ and $So_M = \{o_M\}$;

(d) M is faithful;

(e) There is a mapping $\underline{\varepsilon} : N = M \setminus \{o_M\} \to S$ such that $\underline{\varepsilon}(x)y = 0_M$ and $\underline{\varepsilon}(x)z = o_M$ for all $x \in N$, $y, z \in M$, $y \leq x$, $z \not\leq x$.

Throughout this section, let M be a characteristic semimodule and $L = M \setminus \{0_M\}$.

3.1 Lemma. (i) *$\underline{\varepsilon}$ is an injective mapping of N into R.*
(ii) *$|R| \geq 2$ and $R = \{\, a \in S \mid aM = \{0_M, o_M\} \,\}$.*
(iii) *$o_S \in S$, $o_R \in R$ and $o_S = o_R = \underline{\varepsilon}(0_M)$.*
(iv) *$o_S L = \{o_M\}$.*

Proof. (i) We have $a\underline{\varepsilon}(x)y = \underline{\varepsilon}(x)y$ for all $a \in S$, $x \in N$ and $y \in M$ (use (e), (b) and (c)). Since M is faithful, we get $\underline{\varepsilon}(x) \in R$. If $\underline{\varepsilon}(x_1) = \underline{\varepsilon}(x_2)$ then $0_M = \underline{\varepsilon}(x_1)x_1 = \underline{\varepsilon}(x_2)x_1$ and $x_1 \leq x_2$. By symmetry, we obtain $x_1 = x_2$.
(ii) Since $|N| \geq 2$ due to (a), we get $|R| \geq 2$ due to (i). If $a \in R$ and $x \in M$ are such that $ax \in N$ then $ax = \underline{\varepsilon}(ax)ax = 0_M$. Thus $aM = \{0_M, o_M\}$. Conversely, if $a \in S$ is such that $aM = \{0_M, o_M\}$ then $bax = ax$ for all $b \in S$ and $x \in M$. Since M is faithful, we get $ba = a$ and $a \in R$.
(iii) $(\underline{\varepsilon}(0_M) + a)x = \underline{\varepsilon}(0_M)x + ax = o_M + ax = o_M = \underline{\varepsilon}(0_M)x$ for every $x \in L$. Of course, $(\underline{\varepsilon}(0_M) + a)0_M = 0_M = \underline{\varepsilon}(0_M)0_M$. Thus $\underline{\varepsilon}(0_M) + a = \underline{\varepsilon}(0_M)$ and $\underline{\varepsilon}(0_M) = o_S$.
(iv) If $x \in L$ then $o_S x = \underline{\varepsilon}(0_M)x = o_M$. □

3.2 Lemma. *The following conditions are equivalent for $a \in S$:*

(i) $a = 0_S \in S$.

(ii) $a = 0_R \in R$.

(iii) $a + \underline{\varepsilon}(x) = \underline{\varepsilon}(x)$ *for every* $x \in M \setminus \{o_M\}$.

(iv) $aN = \{0_M\}$.

Moreover, if $o_N \in N$ then these conditions are equivalent to:

(v) $ao_N = 0_M$.

Proof. (i) implies (iii) and (ii) implies (iii) trivially, and, evidently, (iv) is equivalent to (v). Now, we show that (iii) implies (iv). Indeed, $0_M = \underline{\varepsilon}(x)x = (\underline{\varepsilon}(x) + a)x = \underline{\varepsilon}(x)x + ax = ax$ for every $x \in N$. On the other hand, if (iv) is true then $a \in R$ by 3.1(ii) and $(a + b)x = ax + bx = 0_M + bx = bx$ for all $b \in S$ and $x \in N$. Then $(a+b)y = by$ for every $y \in M$, $a+b = b$ and $a = 0_S = 0_R$. □

3.3 Lemma. *Let $0_S \in S$. Then:*
(i) $0_S = 0_R \in R$.
(ii) $N + N = N$.
(iii) $0_S = \underline{\varepsilon}(w)$ *for* $w \in N$ *iff* w *is the greatest element of* N.

Proof. (i) See 3.2.
(ii) If $x, y \in N$ then $0_S(x+y) = 0_Sx+0_Sy = 0_M$ by 3.2(iv). Hence $x+y \neq o_M$.
(iii) If $0_S = \underline{\varepsilon}(w)$ then $\underline{\varepsilon}(w)x = 0_Sx = 0_M$ and $x \leq w$ for every $x \in N$. Conversely, if w is the greatest element of N then $\underline{\varepsilon}(w)N = \{0_M\}$ and $\underline{\varepsilon}(w) = 0_S$ by 3.2. □

3.4 Lemma. *The following conditions are equivalent:*

(i) $0_S \in S$ *and* $0_S \in \underline{\varepsilon}(N)$.

(ii) $0_R \in R$ *and* $0_R \in \underline{\varepsilon}(N)$.

(iii) *The set N has the greatest element (if w is that element then $\underline{\varepsilon}(w) = 0_S = 0_R$).*

Proof. See 3.2 and 3.3. □

3.5 Lemma. (i) *If $a \in S$ and $x \in M$ then $ax = 0_M$ iff $x \in N$ and $a \leq \underline{\varepsilon}(x)$.*
(ii) *If $x, y \in N$ then $x \geq y$ iff $\underline{\varepsilon}(x) \leq \underline{\varepsilon}(y)$.*

Proof. It is easy. □

3.6 Lemma. *The semimodule M is simple.*

Proof. Let α be a congruence of M. If $(0_M, o_M) \in \alpha$ then $\alpha = M \times M$. If $(x, o_M) \in \alpha$ for some $x \in N$ then $(0_M, o_M) = (\underline{\varepsilon}(x)x, \underline{\varepsilon}(x)o_M) \in \alpha$. If $x, y \in N$ are such that $x \not\leq y$ and $(x, y) \in \alpha$ then $(0_M, o_M) = (\underline{\varepsilon}(y)y, \underline{\varepsilon}(y)x) \in \alpha$. □

3.7 Lemma. *The right semimodule R_S is faithful.*

Proof. If $a, b \in S$, $a \neq b$, then $ax \neq bx$ for at least one $x \in M$ and we can assume that $bx \not\leq ax$. Then $ax \in N$, $c = \underline{\varepsilon}(ax) \in R$ and $cax = 0_M \neq o_M = cbx$. Thus $ca \neq cb$. □

3.8 Lemma. *Let $a \in R$ and $A = \{ x \in M \mid ax = 0_M \}$. Then:*
(i) *$0_M \in A$, $o_M \notin A$ and A is a subsemilattice of $M(+)$.*
(ii) *If $v \in M$ then $a = \underline{\varepsilon}(v)$ iff $v = o_A \in A$.*

Proof. (i) This is obvious.
(ii) If $a = \underline{\varepsilon}(v)$ then $v \in A$ and, if $y \not\leq v$, then $ay = o_M$ implies $y \notin A$. Thus $v = o_A \in A$. Conversely, if $v = o_A \in A$ then $ax = \underline{\varepsilon}(v)x$ for every $x \in M$ (use 3.1(ii)). Since ${}_SM$ is faithful, we get $a = \underline{\varepsilon}(v)$. □

3.9 Lemma. *Assume that every infinite strictly increasing sequence of elements from M (or N, $K = N \setminus \{0_M\}$) is upwards cofinal in N (K). Put $R_1 = R \setminus \{0_S\}$ ($R_1 = R$ if $0_S \notin S$). Then $R_1 \subseteq \underline{\varepsilon}(N) \subseteq R$.*

Proof. First, observe that if $x_1 < x_2 < x_3 < \dots$ is a sequence of elements from M then $x_i \in K$ for every $i \geq 2$. Next, if $a \in R_1$ then $A = \{ x \in M \mid ax = 0_M \} \subsetneqq N$ by 3.2(iv). Consequently, using our assumption, we get $o_A \in A$ and $a = \underline{\varepsilon}(o_A)$ by 3.8. □

3.10 Lemma. *If every infinite strictly decreasing sequence of elements from R is downwards cofinal in R_1 then every infinite strictly increasing sequence of elements from M is upwards cofinal in $N \setminus \{o_N\}$.*

Proof. If $x_1 < x_2 < x_3 < \dots$ is a sequence of elements from M then $x_i \in N$ for every $i \geq 1$ and $\underline{\varepsilon}(x_1) > \underline{\varepsilon}(x_2) > \underline{\varepsilon}(x_3) > \dots$ by 3.5(ii) and 3.1(i). If, moreover, $x \in N \setminus \{o_N\}$ then $\underline{\varepsilon}(x) \neq 0_S$, and hence $\underline{\varepsilon}(x_j) \leq \underline{\varepsilon}(x)$ and $x \leq x_j$ for some $j \geq 1$. □

3.11 Lemma. *If every infinite strictly increasing sequence of elements from R is upwards cofinal in $R_2 = R \setminus \{o_S\}$ then every infinite strictly decreasing sequence of elements from M is downwards cofinal in $L = M \setminus \{0_M\}$.*

Proof. If $x_1 > x_2 > x_3 > \dots$ is a sequence of elements from M then $x_i \in K = M \setminus \{0_M, o_M\}$ for every $i \geq 2$ and $\underline{\varepsilon}(x_2) < \underline{\varepsilon}(x_3) < \dots$ by 3.5(ii) and 3.1(i). If, moreover, $x \in L$ then $\underline{\varepsilon}(x) \neq o_S$, and hence $\underline{\varepsilon}(x) \leq \underline{\varepsilon}(x_j)$ and $x_j \leq x$ for some $j \geq 1$. □

3.12 Lemma. *Assume that $R_1 \subseteq \underline{\varepsilon}(N)$. Then:*
(i) *If every infinite strictly decreasing sequence of elements from M is downwards cofinal in K then every infinite strictly increasing sequence of elements from R is upwards cofinal in R_2.*
(ii) *If every infinite strictly increasing sequence of elements from M is upwards cofinal in K then every infinite strictly decreasing sequence of elements from R is downwards cofinal in R_1.*

Proof. (i) Let $a_1 < a_2 < a_3 < \dots$ be a sequence of elements from R. Then $a_i \in R_3 = R \setminus \{0_S, o_S\}$ for every $i \geq 2$ and $a_i = \underline{\varepsilon}(x_i)$, where $x_i \in K$. We have $x_2 > x_3 > x_4 > \dots$ and if $a \in R_3$ then $a = \underline{\varepsilon}(x)$, $x \in K$, $x \geq x_j$ and $a \leq a_j$ for some $j \geq 2$.
(ii) Let $a_1 > a_2 > a_3 > \dots$ be a sequence of elements from R. Then $a_i \in R_1$ for every $i \geq 1$ and $a_i = \underline{\varepsilon}(x_i)$, $x_i \in N$, $x_1 < x_2 < x_3 < \dots$. If $a \in R_1$ then $a = \underline{\varepsilon}(x)$, $x \in N$, $x \leq x_j$ and $a_j \leq a$ for some $j \geq 1$. □

For $x \in M$, define a relation ν_x on S by $(a, b) \in \nu_x$ iff $acx = bcx$ for every $c \in S$.

3.13 Lemma. (i) *ν_x is a congruence of the semiring S.*
(ii) *$\nu_x \cap (R \times R)$ is a congruence of the right semimodule R_S.*
(iii) *$R \times R \subseteq \nu_x$ iff $Sx \subseteq \{0_M, o_M\}$.*
(iv) *If $Sx \subseteq \{0_M, o_M\}$ then $\nu_x = S \times S$.*
(v) *$\nu_x = S \times S$ iff $R \times R \subseteq \nu_x$.*
(vi) *If $x \in K$ then $\nu_x = S \times S$ iff $Sx = \{0_M, o_M\}$.*
(vii) *$0_M, o_M \in P(M) = \{\, x \in M \mid Sx \subseteq \{0_M, o_M\} \,\}$ and $P(M)$ is a subsemimodule of M.*

Proof. (i) and (ii). Easy to check.
(iii) If $R \times R \subseteq \nu_x$ then $acx = o_S cx = \underline{\varepsilon}(0_M)cx$ for all $a \in R$ and $c \in S$. If $cx \neq 0_M$ then $acx = o_M$. If, moreover, $cx \in N$ then $o_M = \underline{\varepsilon}(cx)cx = 0_M$, a contradiction. Thus $cx = o_M$ and we see that $Sx \subseteq \{0_M, o_M\}$.
(iv) and (v). Use (iii).
(vi) If $x \in K$ then $\underline{\varepsilon}(x)x = 0_M$ and $o_S x = \underline{\varepsilon}(0_M)x = o_M$.
(vii) Easy to check. □

3.14 Remark. Assume that the right semimodule R_S is simple (cf. 2.10). If $x \in M$ is such that $Sx \not\subseteq \{0_M, o_M\}$ then $R \times R \not\subseteq \nu_x$, and hence $x \in K$ and $\nu_x \cap (R \times R) = \mathrm{id}_R$. Now, if $a, b \in R$ are such that $a < b$ then $acx = 0_M$ and $bcx = o_M$ for some $c \in S$ (see 3.1(ii)). Consequently, $cx \in K$, $ac \leq \underline{\varepsilon}(x)$ (see 3.5(i)) and $\underline{\varepsilon}(x) = ac + \underline{\varepsilon}(x) < bc + \underline{\varepsilon}(x) \in R$.

3.15 Remark. Assume that the left R-semimodule ${}_R S$ is not faithful. Then there are $a, b \in R$ such that $a < b$ and $ac = bc$ for every $c \in S$.
(i) Let $a = \underline{\varepsilon}(x)$ and $b = \underline{\varepsilon}(y)$, $x, y \in N$. Then $y < x$ and $\underline{\varepsilon}(x)cz = acz = bcz = \underline{\varepsilon}(y)cz$ for every $z \in M$. In particular, if $cz \leq x$ then $cz \leq y$. Since $y < x$, it follows that $x \notin SM$. In fact, $x \neq c_1x_1 + \dots + c_nx_n$ for all $n \geq 1$, $c_i \in S$, $x_i \in M$, and the same is true for x' such that $y < x' \leq x$.
(ii) Let $a = 0_S$ and $b = \underline{\varepsilon}(y)$, $y \in N$. Then $y \in K$ and $0_S cz = \underline{\varepsilon}(y)cz$ for every $z \in M$. In particular, if $cz \in N$ then $cz \leq y$. Consequently, for all $n \geq 1$, $c_i \in S$ and $x_i \in M$, either $x = c_1x_1 + \dots + c_nx_n \leq y$ or $x = o_M$.
(iii) If the semiring S is simple then $ce = de$ for all $c, d, e \in S$. Consequently, $|S| = 2$ and $S = R$.

Consider the following two conditions:

(f1) For all $a, b \in R$, $a \neq b$ ($a < b$) and $x \in K$ there is at least one $c \in S$ with $acx \neq bcx$ (then $acx = 0_M$ and $bcx = o_M$).

(f2) $K \subseteq Sx$ for every $x \in K$.

3.16 Lemma. (f2) *implies* (f1).

Proof. Since ${}_SM$ is faithful, there is $y \in M$ such that $ay \neq by$. Clearly, $y \in K$, and if (f2) is true then $y = cx$, $c \in S$. Thus $acx \neq bcx$. □

3.17 Lemma. *Assume that the right semimodule R_S is simple. Then* (f1) *is equivalent to $Sx \cap K \neq \emptyset$ for every $x \in K$.*

Proof. If (f1) is true and $x \in K$ then $\nu_x \cap (R \times R) = \mathrm{id}_R$, and hence $Sx \not\subseteq \{0_M, o_M\}$ by 3.13(iii). Conversely, if $Sx \cap K \neq \emptyset$ then $R \times R \not\subseteq \nu_x$ and, R_S being simple, we get $\nu_x \cap (R \times R) = \mathrm{id}_R$. □

3.18 Lemma. *Let the set K contain the smallest element, say w, and let $Sw \not\subseteq \{0_M, o_M, w\}$. If $c \in S$ is such that $cw \notin \{0_M, o_M, w\}$ then $\underline{\varepsilon}(w)c = o_S$, $\underline{\varepsilon}(w) \neq o_S \neq c$ and $c \notin R$.*

Proof. Since $cw \in K$, we have $c \notin R$, and hence $c \neq o_S$ (use 3.1(ii)). Since $w \neq 0_M$, we have $\underline{\varepsilon}(w) \neq o_S$. Now, if $y \in L = M \setminus \{0_M\}$ then $w \leq y$, and hence $o_M = \underline{\varepsilon}(w)cw \leq \underline{\varepsilon}(w)cy$ (we have $w < cw$). Consequently, $\underline{\varepsilon}(w)cx = o_S x$ for every $x \in M$ and we get $\underline{\varepsilon}(w)c = o_S$. □

3.19 Lemma. *Let $|R| \geq 3$ and let the set K contain the smallest element. If the condition* (f1) *is satisfied then $o_S = ac$ for some $a \in R_2 = R \setminus \{o_S\}$ and $c \in S \setminus R$.*

Proof. Let w be the smallest element in K. Since $|R| \geq 3$, there are $a, b \in R$ such that $a \neq b$ and $aw = bw$ (use 3.1(ii)). Now, by (f1), there is $c \in S$ such that $acw \neq bcw$. Then $cw \notin \{0_M, o_M, w\}$ and 3.18 applies. □

3.20 Remark. If $|R| = 2$ and (f1) is true then $|S| = 3$, $1_S \in S$ and $o_S \neq 0_S = ac$ for all $a \in R \setminus \{o_S\} = \{0_S\}$ and $c \in S \setminus R = \{1\}$.

3.21 Lemma. *$o_S \in R_2 + R_2$ in each of the following cases:*

1. *The set K has at least one minimal element but no smallest element.*
2. *The set R_2 has at least one maximal element but no greatest element.*
3. *There are $u, v \in K$ such that, for every $x \in K$, either $x \not\leq u$ or $x \not\leq v$.*

Proof. (i) Let $w \in K$ be minimal. Since w is not the smallest element of K, there is $v \in K$ with $w \not\leq v$. If $x \in K$ is such that $x \leq v$ then $x \not\leq w$, and hence $(\underline{\varepsilon}(w) + \underline{\varepsilon}(v))x = o_M$. If $x \not\leq v$ then $(\underline{\varepsilon}(w) + \underline{\varepsilon}(v))x = o_M$ as well. Thus $\underline{\varepsilon}(w) + \underline{\varepsilon}(v) = \underline{\varepsilon}(0_M) = o_S$.
(ii) If a is maximal in R_2 then $b \not\leq a$ for some $b \in R_2$, and so $a + b = o_S$. □

3.22 Remark. Let $b \in S \setminus R$ be such that the set bM is finite. Due to 3.1(ii), we have $bM = \{0_M, w_1, \ldots, w_n, o_M\}$, where $n \geq 1$ and $w_i \in K$. Put $w = w_1 + \cdots + w_n$. There are $u_1, \ldots, u_n \in K$ such that $w_i = bu_i$, Then $w = bu$, $u = u_1 + \cdots + u_n$.
(i) If $n = 1$ or $N + N = N$ then $w \in K$.
(ii) Assume that $w \in K$. Then $w = w_j$ for some $1 \leq j \leq n$. If $a = \underline{\varepsilon}(w)$ then $a \in R_2$, $abx = 0_M$ for $x \in M$, $bx \in N$, and $aby = o_M$ for $y \in M$, $by = o_M$.
(iii) Let $w \in K$ and $bN \subseteq N$. Then $bN \leq w$, $abN \leq aw = 0_M$ and $ab = 0_S \in S$ by 3.2(iv). Since $b \notin R$, we have $b \neq 0_S$. On the other hand, $a = 0_S$ iff w is the greatest element of N.
(iv) If $w \in K$, w is not the greatest element of N and $bN \subseteq N$ then $a \neq 0_S \neq b$ and $ab = 0_S$.
(v) Assume that $bL \subseteq L$, $L = M \setminus \{0_M\}$. If $v \in K$ is such that $v < w_i$ for every $i = 1, \ldots, n$ and if $\overline{a} = \underline{\varepsilon}(v)$ then $\overline{a} \neq o_S$ and $\overline{a}bx = o_M$ for every $x \in L$. Thus $\overline{a}b = o_S$. Of course, $b \notin R$, and so $b \neq o_S$ as well.

3.23 Remark. Let $v \in K$, $a = \underline{\varepsilon}(v)$ and $b \in S$. We have $a \in R_2$.
(i) If $bN \leq v$ then $abN = \{0_M\}$, and hence $ab = 0_S \in S$ by 3.2. Conversely, if $ab = 0_S \in S$ then $bN \leq v$.
(ii) Let $ab = 0_S \in S$. If $x, y \in N$ are such that $bx \not\leq by \neq 0_M$ then $b \neq 0_S$, $\underline{\varepsilon}(by)bx = o_M$, $\underline{\varepsilon}(by)b \neq 0_s, o_S$ and $\underline{\varepsilon}(by) \neq o_S$. Of course, $a = \underline{\varepsilon}(v) < \underline{\varepsilon}(by)$, $by < v$ and $\underline{\varepsilon}(by) \in R_3 = R \setminus \{0_S, o_S\}$. If $a \neq 0_S$ (equivalently, $v \neq o_N$) then $(a, \underline{\varepsilon}(by)) \in R_3 \times R_3$ and $(ab, \underline{\varepsilon}(by)b) = (0_S, \underline{\varepsilon}(by)b) \notin R_3 \times R_3$. In particular, the relation $\alpha_3 = (R_3 \times R_3) \cup \mathrm{id}_R$ is not a congruence of the right semimodule R_S. Similarly, $\alpha_1 = (R_1 \times R_1) \cup \mathrm{id}_R$, where $R_1 = R \setminus \{0_S\}$, is not a congruence of R_S.
(iii) Let $ab = 0_S \neq b$ and let $bx \leq by$ for all $x, y \in N$ such that $by \neq 0_M$. Now, $bx_1 = by_1$ whenever $bx_1 \neq 0_M \neq by_1$, $x_1, y_1 \in N$. Since $ab = 0_S \neq b$, we have $b \notin R$, and hence there is $w \in K$ such that $bM = \{0_M, w, o_M\}$, $bN = \{0_M, w\}$ and $\underline{\varepsilon}(w)b = 0_S$ (cf. 3.22(iv)).

If $bw = 0_M$ then $(b + \underline{\varepsilon}(w))z = \underline{\varepsilon}(w)z$ for every $z \in M$, so that $b \leq \underline{\varepsilon}(w)$, $b^2 = 0_S \neq \underline{\varepsilon}(w)$ and $w \neq o_N$. We have $bN \leq v$, and so $w \leq v$, $a = \underline{\varepsilon}(v) \leq \underline{\varepsilon}(w)$.

If $bw \neq 0_M$ then $bw = w$, and so $bz = b^2z$ for every $z \in M$ and we get $b^2 = b$.

3.24 Remark. Assume that the condition (f1) is satisfied.
(i) If $u, v \in N$ are such that $u < v$ then $\underline{\varepsilon}(v) < \underline{\varepsilon}(u)$, and hence for every $x \in K$ there is $c \in S$ with $cx \leq v$ and $cx \not\leq u$. In particular, if $u = 0_M$ and $v \neq o_M$ then $cx \in K$. If v is minimal in K (and $u = 0_M$) then we get $cx = v$.
(ii) If v is minimal in K then $v \in Sx$ for every $x \in K$.

(iii) If $K \subseteq Sv$ for a minimal element $v \in K$ then (f2) is true.
(iv) Let A denote the subsemimodule of ${}_SM$ generated by $0_M, o_M$ and all minimal elements from K. Then $A \subseteq Sx$ for every $x \in K$. Thus (f2) is true, provided that $A = M$.
(v) (cf. 3.19) Assume that the set K contains the smallest element w. If $a, b \in R$ are such that $a < b$ then $acw = 0_M$ and $bcw = o_M$ for some $c \in S$. Since $cw \neq o_M$, we have $c \neq o_S$. Furthermore, $bcw = o_M$ implies $bcL = \{o_M\}$, where $L = M \setminus \{0_M\}$, and hence $bc = o_S$. Of course, $c \notin R$ follows from 3.1(ii). If $|R| \geq 3$ then we can choose $b \neq o_S$.
(vi) Assume that $o_N \in N$. If $a, b \in R$ are such that $a < b$ then $aco_N = 0_M$ and $bco_N = o_M$ for some $c \in S$. Since $co_N \neq 0_M$, we have $c \neq 0_S$. Furthermore, $aco_N = 0_M$ implies $acN = \{0_M\}$ and $ac = 0_S$ (see 3.2(iv)). If $|R| \geq 3$ then we can choose $a \neq 0_S$.

4. Auxiliary results (c)

Let S be a semiring and M ($=_S M$) a characteristic (left S-)semimodule (see the preceding section). Furthermore, let α be a congruence of the semimodule R_S such that $\alpha \neq \mathrm{id}_R$ and $\alpha \neq R \times R$. We put $A = \{\, a \in R \mid (a, o_S) \notin \alpha \,\}$ and $B = R \setminus A$. Thus $B = \{\, b \in R \mid (b, o_S) \in \alpha \,\}$ is just the block of α containing the absorbing element o_S and we have $A \neq \emptyset$. If $0_S \in S$ then $0_S \in A$.

4.1 Lemma. *Assume that the set A has no maximal element. Then:*
(i) *There is an infinite strictly increasing sequence $a_1 < a_2 < a_3 < \dots$ of elements from A.*
(ii) *If $b \in B$ and $i \geq 1$ then $b \not\leq a_i$.*

Proof. If $b \leq a_i$ then $(a_i, o_S) = (a_i + b, a_i + o_S) \in \alpha$, a contradiction. □

4.2 Lemma. *Let $a_0 \in R \setminus \underline{\varepsilon}(N)$. Then:*
(i) $0_M \in C = \{\, x \in M \mid a_0 x = 0_M \,\}$ *and $C(+)$ is a subsemilattice of $M(+)$.*
(ii) *The set C has no maximal element.*
(iii) $a_0 < \underline{\varepsilon}(x)$ *for every $x \in C$.*
(iv) *If $C = N$ then $a_0 = 0_S \in S$.*

Proof. If $v \in C$ is maximal in C then $v = o_C \in C$, $\underline{\varepsilon}(v)x = 0_M = a_0 x$ for $x \leq v$ and $\underline{\varepsilon}(v)y = o_M$ for $y \not\leq v$. But $y \not\leq v$ means $y \notin C$, $a_0 y \neq 0_M$ and $a_0 y = o_M$ by 3.1(ii). Thus $\underline{\varepsilon}(v)z = a_0 z$ for every $z \in M$ and $\underline{\varepsilon}(v) = a_0$, a contradiction By 3.5(i), we get $a_0 < \underline{\varepsilon}(x)$ for every $x \in C$. If $C = N$ then $a_0 N = \{0_M\}$ and $a_0 = 0_S$ by 3.2. □

4.3 Lemma. *Let $a_0 \in R \setminus \underline{\varepsilon}(N)$. Then:*
(ii) *There is an infinite strictly increasing sequence $x_1 < x_2 < x_3 < \dots$ of elements from C.*
(ii) *If $u \in M \setminus C$ then $u \not\leq x_i$ for every $i \geq 1$.*

(iii) $\underline{\varepsilon}(x_1) > \underline{\varepsilon}(x_2) > \underline{\varepsilon}(x_3) > \dots$ *is an infinite strictly decreasing sequence of elements from* R *such that* $\underline{\varepsilon}(x_i) > a_0$ *for every* $i \geq 1$.

Proof. Use 4.2 and 3.5(ii). □

4.4 Lemma. *If* a_0 *is maximal in* A *then* $(a_0, a) \notin \alpha$ *for every* $a \in R$ *such that* $a_0 < a$.

Proof. We have $a \notin A$, $(a, o_S) \in \alpha$, and hence $(a_0, a) \notin \alpha$. □

4.5 Lemma. *Let* $a, b \in R$, $c \in S$ *and* $x \in M$ *be such that* $(a, b) \in \alpha$, $a < b$ *and* $acx \neq bcx$. *Then* $x \in K$, $\underline{\varepsilon}(x) < bc + \underline{\varepsilon}(x) = \overline{a} \in R$ *and* $(\underline{\varepsilon}(x), \overline{a}) \in \alpha$.

Proof. Since $acx \neq bcx$, we have $acx = 0_M$ and $bcx = o_M$ by 3.1(ii). Consequently, $x, cx \in K$ and $(ac+\underline{\varepsilon}(x))y \leq (ac+\underline{\varepsilon}(x))x = acx+\underline{\varepsilon}(x)x = 0_M$ for $y \leq x$. On the other hand, if $z \not\leq x$ then $(ac + \underline{\varepsilon}(x))z = o_M$. Then $ac + \underline{\varepsilon}(x) = \underline{\varepsilon}(x)$ and $ac \leq \underline{\varepsilon}(x)$. Furthermore, $(\underline{\varepsilon}(x), \overline{a}) = (ac+\underline{\varepsilon}(x), bc+\underline{\varepsilon}(x)) \in \alpha$ and $\underline{\varepsilon}(x) \leq \overline{a}$. Since $\overline{a}x = bcx + \underline{\varepsilon}(x)x = o_M \neq 0_M = \underline{\varepsilon}(x)x$, we conclude that $\underline{\varepsilon}(x) < \overline{a}$. □

4.6 Lemma. *Assume that* (f1) *is true. Then for every* $x \in K$ *there is* $\overline{a} \in R$ *with* $\underline{\varepsilon}(x) < \overline{a}$ *and* $(\underline{\varepsilon}(x), \overline{a}) \in \alpha$.

Proof. Since $\alpha \neq \mathrm{id}_R$, there are $a, b \in R$ with $a < b$ and $(a, b) \in \alpha$. By (f1), $acx \neq bcx$ for some $c \in S$. The rest follows from 4.5. □

4.7 Lemma. *Assume that* (f1) *is true. If* a_0 *is maximal in* A *then* $a_0 \notin \underline{\varepsilon}(N)$.

Proof. Since $a_0 \in A$, we have $a_0 \neq o_S = \underline{\varepsilon}(0_M)$. The rest is clear from 4.4 and 4.6. □

4.8 Lemma. *Aassume that* (f1) *is true and* $A \setminus \{0_S\} \subseteq \underline{\varepsilon}(N)$. *If* $a \in A \setminus \{0_S\}$ *then:*
(i) *There is an infinite strictly increasing sequence* $a = a_1 < a_2 < a_3 < \dots$ *of elements from* A *such that all these elements belong to the same block of the congruence* α.
(ii) *If* $b \in B$ *then* $b \not\leq a_i$ *for every* $i \geq 1$.
(iii) *There is an infinite strictly decreasing sequence* $x_1 > x_2 > x_3 > \dots$ *of elements from* K *such that* $a_i = \underline{\varepsilon}(x_i)$ *for every* $i \geq 1$.
(iv) *If* $x \in N$ *is such that* $x \geq x_j$ *for some* $j \geq 1$ *(equivalently,* $\underline{\varepsilon}(x) \leq a_j$*) then* $\underline{\varepsilon}(x) \in A$.

Proof. We have $a_1 = a = \underline{\varepsilon}(x_1)$ for some $x_1 \in K$. By 4.6, there is $a_2 \in R$ with $a_1 < a_2$ and $(a_1, a_2) \in \alpha$. Clearly, $a_2 \in A \setminus \{0_S\}$, and so $a_2 = \underline{\varepsilon}(x_2)$ for some $x_2 \in K$. Now, $x_1 > x_2$ and we can proceed in this way on. □

4.9 Lemma. *Assume that* (f1) *is true and* $A \setminus \{0_S\} \subseteq \underline{\varepsilon}(N)$. *If the set* A *has at least one maximal element then* $0_S \in S$, $A = \{0_S\}$ *and* $B = R \setminus \{0_S\}$.

Proof. If a_0 is maximal in A then $a_0 \notin \underline{\varepsilon}(N)$ by 4.7, and hence $a_0 = 0_S \in S$. Since 0_S is maximal in A, we have $A = \{0_S\}$ and $B = R \setminus \{0_S\}$. □

5. Auxiliary results (d)

In this section, let S be a semiring such that $R = \underline{R}(S) \neq \emptyset$.

5.1 Lemma. Assume that $0_S \in S$ and the right semimodule R_S is faithful. Then $0_S = 0_R \in R$ and the following conditions are equivalent:

(i) $\alpha_1 = (R_1 \times R_1) \cup \mathrm{id}_R$, where $R_1 = R \setminus \{0_S\}$, is a congruence of R_S.

(ii) $ab \neq 0_S$ for all $a \in R_1$ and $b \in S_1 = S \setminus \{0_S\}$.

(iii) $cd \neq 0_S$ for all $c, d \in S_1$.

(iv) Either $|S| = 1$ or S_1 is a subsemiring of S.

Proof. Proceeding similarly as in the proof of 2.2(i), we show that $0_S = 0_R \in R$. Now, if α_1 is a congruence of R_S and if $ab = 0_S$ for some $a \in R_1$ and $b \in S_1$ then $(0_S, a'b) = (ab, a'b) \in \alpha_1$ for every $a' \in R_1$ and it follows that $a'b = 0_S$. Thus $R_1 b = \{0_S\}$. Since $0_S b \leq ab = 0_S$, we have $Rb = \{0_S\}$. Of course, $R0_S \leq Rb$, and therefore $Rb = \{0_S\} = R0_S$. Since R_S is faithful, we conclude that $b = 0_S$, a contradiction. We have proved that $ab \neq 0_S$. If $cd = 0_S$ for some $c, d \in S_1$ then $ec \neq e0_S = 0_S$ for some $e \in R$ and we have $ec \in R_1$ and $ecd = e0_S = 0_S$. The rest is clear. □

5.2 Lemma. Assume that $o_S \in S$ and the right semimodule R_S is faithful. Then $o_S = o_R \in R$ and the following conditions are equivalent:

(i) $\alpha_2 = (R_2 \times R_2) \cup \mathrm{id}_R$, where $R_2 = R \setminus \{o_S\}$, is a congruence of R_S.

(ii) $a + b \neq o_S \neq ac$ for all $a, b \in R_2$ and $c \in S_2 = S \setminus \{o_S\}$.

(iii) Either $|S| = 1$ or S_2 is a subsemiring of S.

Proof. We can proceed similarly as in the proof of 5.1. □

5.3 Remark. Assume that $o_S \in S$, the semimodule R_S is faithful and $o_S \notin R_2 S_2$. Assume, furthermore, that the set R_2 has no maximal element and that α_2 is not a congruence of R_S. Then $\alpha_2 \neq \mathrm{id}_R$, R is infinite and, by 5.2, $a + b = o_S$ for some $a, b \in R_2$. Moreover, there is an infinite strictly increasing sequence $a = a_1 < a_2 < a_3 < \dots$ of elements from R_2. Since $a + b = o_S$, we have $b \not\leq a_i$ for every $i \geq 1$.

5.4 Remark. Assume that $o_S \in S$ ($0_S \in S$) and $o_S \in R$ ($0_S \in R$) (cf. 2.1, 2.2, 2.3 and 2.4). Put $A = \{\, a \in S \mid o_S a = o_S \,\}$ ($A = \{\, a \in S \mid 0_S a = 0_S \,\}$) and $B = S \setminus A$. Clearly, $o_S \in A$ ($0_S \in A$), A is a subsemiring of S, $A + S = A$ ($B + S = B$) and $SB \subseteq B$. Further, put $\beta = (A \times A) \cup (B \times B)$.
(i) $\beta = \mathrm{id}_S$ iff $|S| = 1, 2$.
(ii) $\beta = S \times S$ iff o_S (0_S) is multiplicatively absorbing (equivalently, $|R| = 1$).
(iii) If $S_2 = S \setminus \{o_S\}$ is a subsemiring of S then β is a congruence of the semiring S.
(iv) If $|S| \geq 3$, $|R| \geq 2$ and S is a simple semiring then S_2 is not a subsemiring of S (cf. 5.2 and 2.10).

5.5 Proposition. *Assume that $|R| \geq 3$ and the right semimodule R_S is both faithful and simple* (cf. 2.10). *Then:*
(i) *If $0_S \in S$ then $0_S \in R$ and $ab = 0_S$ for some $a \in R_1$ and $b \in S_1$.*
(ii) *If $o_S \in S$ then $o_S \in R$ and either $a + b = o_S$ for some $a, b \in R_2$ or $cd = o_S$ for some $c \in R_2$ and $d \in S_2$.*

Proof. Use 5.1 and 5.2. □

6. Main results

Let S be a semiring and M ($=_S M$) be a characteristic (left S-) semimodule (in particular, $|M| \geq 3$ and $|S| \geq |R| \geq 2$). Put $N = M \setminus \{o_M\}$, $L = M \setminus \{0_M\}$, $K = M \setminus \{0_M, o_M\}$, $R_1 = R \setminus \{0_S\}$, $R_2 = R \setminus \{o_S\}$ and $R_3 = R \setminus \{0_S, o_S\}$. Consider the following four conditions:

(g1) Any infinite strictly increasing sequence of elements from K is upwards cofinal in K.

(g2) Any infinite strictly decreasing sequence of elements from K is downwards cofinal in K.

(h1) Any infinite strictly increasing sequence of elements from R_3 is upwards cofinal in R_3.

(h2) Any infinite strictly decreasing sequence of elements from R_3 is downwards cofinal in R_3.

6.1 Lemma. (i) *If (g1) is true then (h2) is true.*
(ii) *If (g1) and (g2) are true then (h1) is true.*
(iii) *If (h1) is true then (g2) is true.*

Proof. See 3.9, 3.10, 3.11 and 3.12. □

6.2 Lemma. (i) *If (g1) is true then $R_1 \subseteq \underline{\varepsilon}(N) \subseteq R$.*
(ii) *If (h2) is true and $o_N \notin N$ then (g1) is true.*

(iii) *If (h2) is true and $o_N \in N$ then every infinite strictly increasing sequence of elements from M is upwards cofinal in $N \setminus \{o_N\}$.*

Proof. See 3.9, 3.10, 3.11 and 3.12. □

6.3 Lemma. *Assume that (g1),(g2) or (h1),(h2) are true. Then:*
(i) *If the set K has no minimal element then the ordered set $L(\leq)$ is a lattice and $R_2 + R_2 = R_2$.*
(ii) *If the set K has a minimal element, but no smallest one, then $|M| \geq 4$ and $R_2 + R_2 \neq R_2$ (i.e., $o_S \in R_2 + R_2$).*
(iii) *If the set K has the smallest element then the set R_2 has the greatest element and $R_2 + R_2 = R_2$.*

Proof. (i) Given $x \in L$, there is an infinite strictly decreasing sequence $x = x_1 > x_2 > x_3 > \dots$ of elements from L. If (h1) is true then (g2) is true by 6.1(iii). If (g2) is true and $y \in L$ then $y \geq x_i$ for some $i \geq 1$. Thus the element $x_i \in L$ is a lower bound of elements x and y. Now, put $A = \{\, z \in L \mid z \leq x, z \leq y \,\}$. The set A is non-empty and if $o_A \in A$ then $o_A = \inf(x, y)$. On the other hand, if $o_A \notin A$ and (g1) is true then $N \subseteq A$, and therefore either $x \leq y$ or $y \leq x$, a contradiction with $o_A \notin A$. Finally, if $o_A \notin A$ and (g1) is not true then (h2) is true, $o_N \in N$ and $N \setminus \{o_N\} \subseteq A$ (use 6.2(ii),(iii)). But then $\{x, y\} \subseteq \{o_N, o_M\}$ and we get a contradiction again.

It remains to show that $R_2 + R_2 = R_2$. For, let $a, b \in R_2$ be such that $a + b = o_S$. If $a = \underline{\varepsilon}(u)$ and $b = \underline{\varepsilon}(v)$ for some $u, v \in N$ then $u, v \in K$ and $z \leq u$, $z \leq v$ for some $z \in K$ (since L is a lattice) and $a = \underline{\varepsilon}(u) \leq \underline{\varepsilon}(z)$, $b = \underline{\varepsilon}(v) \leq \underline{\varepsilon}(z)$. Thus $o_S = a + b \leq \underline{\varepsilon}(z) \in R_2$, a contradiction. Therefore, we can assume that $a \notin \underline{\varepsilon}(N)$.

Since $a+b = o_S$ and $a, b \in R_2$, we see that $a, b \in R_1$. According to 6.2(i), the condition (g1) is not true, and hence (h1), (h2) are true and $o_N \in N$ (see 6.2(ii)). By 3.4, $0_S = \underline{\varepsilon}(o_N)$ and, by 3.8, $o_A \notin A = \{\, x \in M \mid ax = 0_M \,\}$. Using 6.2(iii), we conclude that $A = N \setminus \{o_N\}$. Consequently, $(a+b)x = 0_M + bx = bx$ for every $x \in N \setminus \{o_N\}$. Of course, $(a+b)o_M = o_M = bo_M$ and $(a+b)o_N = o_M + bo_N = o_M$. Since $b \neq 0_S = \underline{\varepsilon}(o_N)$, we have $bN \neq \{0_M\}$, and so $bo_N = o_M$. We have proved that $(a + b)y = by$ for every $y \in M$ and, since ${}_SM$ is faithful, it means that $o_S = a + b = b \neq o_S$, the final contradiction.
(ii) Clearly, $|M| \geq 4$ and we use 3.21.
(iii) Let w be the smallest element of K. If $\underline{\varepsilon}(w)$ is the greatest element of R_2 then $R_2 + R_2 = R_2$ trivially. If not then $a \not\leq \underline{\varepsilon}(w)$ for some $a \in R_2$. Then $a \notin \underline{\varepsilon}(N)$ and, since ${}_SM$ is faithful, there is $v \in M$ with $av \not\leq \underline{\varepsilon}(w)v$. Clearly, $v \in K$, $w \leq v$, $av \neq 0_M$, and hence $av = o_M$ (see 3.1(ii)). Since $\underline{\varepsilon}(w)v \neq av = o_M$, we have $\underline{\varepsilon}(w)v = 0_M$, and so $v \leq w$. Thus $w = v$ and $aw = o_M$. We have $a \neq 0_S$ (otherwise $aw \leq \underline{\varepsilon}(w)v$) and it follows from 6.2(i) that (g1) is not true. Using 6.2(ii), we see that $o_N \in N$ and (h2) is true. Besides, it follows from 3.8 and 6.2(ii) that $a(N \setminus \{o_N\}) = \{0_M\}$. Since $aw = o_M$, we get $w = o_N$ and,

w being the smallest element in K, we get $|M| = 3$, $|R| = 2$, $R_2 = \{0_S\}$ and $a = 0_S = \underline{\varepsilon}(w)$, a contradiction. □

6.4 Remark. Let (h2) be true and let $o_N \in N$. If $a \in R \setminus \underline{\varepsilon}(N)$ then a is the smallest element in R_1.

6.5 Lemma. *Assume that (g1),(g2) or (h1),(h2) are true. Then:*
(i) *If the set R_2 has no maximal element then $R_2 + R_2 = R_2$.*
(ii) *If $v \in K$ is minimal in K then $\underline{\varepsilon}(v)$ is maximal in R_2.*
(iii) *If $a \in R_2$ is maximal in R_2 then $a = \underline{\varepsilon}(w)$, where w is minimal in K.*
(iv) *If $a \in R_2$ is maximal, but not the greatest element of R_2 then $R_2 + R_2 \neq R_2$.*
(v) *If $w \in K$ is the smallest element of K then $\underline{\varepsilon}(w)$ is the greatest element of R_2.*
(vi) *If $a \in R_2$ is the greatest element of R_2 then $R_2 + R_2 = R_2$ and $a = \underline{\varepsilon}(w)$, where w is the smallest element of K.*

Proof. (i) By 6.1(ii), the condition (h1) is true and the equality follows easily.
(ii) Let $a \in R$ be such that $\underline{\varepsilon}(v) \leq a$. If $a = \underline{\varepsilon}(u)$, $u \in N$, then $u \leq v$ and either $u = v$ and $a = \underline{\varepsilon}(v)$ or $u = 0_M$ and $a = o_S$. On the other hand, if $a \notin \underline{\varepsilon}(N)$ then $a \neq 0_S$ (otherwise $a = 0_S = \underline{\varepsilon}(v)$) and it follows from 6.2(i),(ii) and 6.4 that a is the smallest element of R_1. Since $\underline{\varepsilon}(v) < a$, we get $\underline{\varepsilon}(v) = 0_S$, $v = o_N$, $|M| = 3$ and (g1) is true. Then $a \in \underline{\varepsilon}(N)$ by 6.2(i), a contradiction.
(iii) If $a \notin \underline{\varepsilon}(N)$ then either $a = 0_S$, $|R| = 2$, $|N| = 3$, a contradiction, or a is the smallest element of R_1, $|R| = 3$, $|M| \leq 3$, a contradiction again. Thus $a \in \underline{\varepsilon}(N)$.
(iv) This is obvious.
(v) By (ii), $\underline{\varepsilon}(w)$ is maximal in R_2. If $a \not\leq \underline{\varepsilon}(w)$, $a \in R_2$, then $a \notin \underline{\varepsilon}(N)$, a contradiction with 6.2(i) and 6.4.
(vi) Clearly, $R_2 + R_2 = R_2$. If $a \notin \underline{\varepsilon}(N)$ then either $a = 0_S$, $|M| = 3$ and $a = \underline{\varepsilon}(o_N)$, a contradiction, or a is the smallest element of R_1, so that $|R| = 3$, $R = \{0_S, a, o_S\}$, $|M| = 3$, (g1) is true and $a \in \underline{\varepsilon}(N)$, a contradiction again. □

In the reamining part of this section, assume that the condition (f1) (see the definition before 3.16) is satisfied and either the conditions (g1),(g2) are true or the conditions (h1),(h2) are true (then, due to 6.1, the conditions (h1), (h2), (g2) are true anyway).

6.6 Theorem. Assume that $0_s \notin S$ (then $o_N \notin N$ – see 3.4). The semiring S is simple if and only if the following two conditions are satisfied:

1. $S = R + S$.
2. Either $o_S \in R_2S_2$ ($o_S \in S_2S_2$, resp.) or the set K contains at least one minimal element (equivalently, the set R_2 has a maximal element).

Proof. (i) Let S be simple. Then $S = R + S$ follows from 2.7 and the right semimodule R_S is simple and faithful (2.4, 2.7 and/or 3.7). Since $0_S \notin S$, we

have $o_N \notin N$ by 3.4, $|N| \geq 3$, $|R| \geq 3$ and $\alpha_2 = (R_2 \times R_2) \cup \mathrm{id}_R \neq \mathrm{id}_R, R \times R$. By 5.2, $o_S \in (R_2 + R_2) \cup R_2S_2$. If K has no minimal element then $o_S \in R_2S_2$ follows from 6.3(i).
(ii) Assume that the conditions (1) and (2) are satisfied. With respect to 2.10, we have to check that the right semimodule R_S is simple. For, let $\alpha \neq \mathrm{id}_R, R \times R$ be a congruence of R_S and $A = \{\, a \in R \,|\, (a, o_S) \notin \alpha \,\}$.

Let $a_0 \in A \setminus \underline{\varepsilon}(N)$. The condition (h2) is true, and hence $a_0 = 0_S \in S$ by 4.3(iii), a contradiction with $0_S \notin S$. It follows that $A \subseteq \underline{\varepsilon}(N)$. By 4.9, the set A has no maximal element.

Let $a, b \in A$. By 4.8(i), there are sequences $a = a_1 < a_2 < a_3 < \dots$ and $b = b_1 < b_2 < b_3 < \dots$ of elements from A such that $(a, a_i) \in \alpha$ and $(b, b_i) \in \alpha$ for every $i \geq 1$. Since (h1) is true, $a \leq b_j$ and $b \leq a_k$ for some $j, k \geq 1$. From this, $(a, b) \in \alpha$ and it means that the set A is contained in a block of α. Furthermore, it follows from 4.8(ii) that $R \setminus A = \{o_S\}$. Consequently, $\alpha = \alpha_2$ and, using (2) and 5.2, we conclude that the set K contains at least one minimal element. We have $R_2 + R_2 = R_2$ (since α_2 is a congruence of R_S), and therefore K has the smallest element by 6.3(ii), a contradiction with 3.19 and 5.2. □

6.7 Theorem. *Assume that $0_S \in \underline{\varepsilon}(N)$ (equivalently, $o_N \in N$). Then the semiring S is simple if and only if the condition* 6.6(2) *is satisfied.*

Proof. (i) Let S be simple. If $|R| \geq 3$ then $\alpha_2 = (R_2 \times R_2) \cup \mathrm{id}_R$ is not a congruence of R_S and 6.6(2) follows from 5.2 and 6.3(i) (see the proof of 6.6). On the other hand, if $|R| = 2$ then $|M| = 3$, $|S| = 3$, $S = \{0_S, 1_S, o_S\}$ and S is not simple ($\{(0_S, 0_S), (0_S, 1_S), (1_S, 0_S), (1_S, 1_S), (o_S, o_S)\}$ is a congruence of S).
(ii) Let the condition 6.6(2) be satisfied. With respect to 2.10, we have to show that R_S is simple. For, let $\alpha \neq \mathrm{id}_R, R \times R$ be a congruence of R_S and $A = \{\, a \in R \,|\, (a, o_S) \notin \alpha \,\}$.

We have $0_S \in A \cap \underline{\varepsilon}(N)$. If $a_0 \in A \setminus \underline{\varepsilon}(N)$ then $a_0 = 0_S$ follows from 4.3(iii) and we see that $A \subseteq \underline{\varepsilon}(N)$. By 4.7, the set A has no maximal element. By 4.6, $(0_S, \overline{a}) \in \alpha$ for at least one $\overline{a} \in R_1$; of course $\overline{a} \in A$. Proceeding similarly as in the proof of 6.6, we show that the set $A \setminus \{0_S\}$ is contained in a block of α. Consequently, the set A is contained in a block of α, $R \setminus A = \{o_S\}$ (see 4.8(ii)) and $\alpha = \alpha_2$. Now, again, we proceed similarly as in the proof of 6.6 to gain the final contradiction. □

6.8 Theorem. Assume that $0_S \in S \setminus \underline{\varepsilon}(N)$ (equivalently, $0_S \in S$ and $o_N \notin N$). Then the semiring S is simple if and only if the conditions 6.6(2) is satisfied and, moreover, the following condition is satisfied as well:

1. $0_S \in R_1S_1 (0_S \in S_1S_1$, resp.).

Proof. (i) Let S be simple. Since $o_N \notin N$, we have $|N| \geq 3$, $|R| \geq 3$ and $\alpha_1, \alpha_2 \neq \mathrm{id}_R, R \times R$ (see 5.1 and 5.2). Since R_S is simple by 2.10, neither α_1 nor α_2 is a congruence of R_S and it remains to use 5.1, 5.2 and 6.3(i).

(ii) Let the conditions (1) and 6.6(2) be satisfied. In view of 2.10, we have to check that the right S-semimodule R_S is simple. For, let $\alpha \neq \mathrm{id}_R, R \times R$ be a congruence of R_S and $A = \{\, a \in R \,|\, (a, o_S) \notin \alpha\}$. Then $|R| \geq 3$, $0_S \in A$, $o_S \notin A$ and it follows from 4.2 and 4.3 that $A' = A \setminus \{0_S\} \subseteq \underline{\varepsilon}(N)$. If $A' = \emptyset$ then $A = \{0_S\}$ and $\alpha = \alpha_1$, a contradiction with (1) and 5.1. It means that $A' \neq \emptyset$. Proceeding similarly as in the proof of 6.6, we find that $A' \times A' \subseteq \alpha$ and $R \setminus A = \{o_S\}$. Thus $A' = R_3$ and $R_3 \times R_3 \subseteq \alpha$.

Assume, for a moment, that $ab = o_S$ for some $a \in R_2$ and $b \in S_2$. If $a = 0_S$ then $Sb = \{o_S\} = So_S$ and $b = o_S$, R_S being faithful, a contradiction. Thus $a \in R_3$ and, since $b \neq o_S$, there is $v \in K$ with $bv \neq o_M$. We have $bv \in N$, $\underline{\varepsilon}(bv)bv = 0_M$ and $\underline{\varepsilon}(bv)b \neq o_S$. If $\underline{\varepsilon}(bv) = o_S$ (i.e., $bv = 0_M$) then $a \leq \underline{\varepsilon}(bv)$ and $o_S = ab \leq \underline{\varepsilon}(bv)b \neq o_S$, a contradiction. Thus $\underline{\varepsilon}(bv) \neq o_S$ and $bv \neq 0_M$. On the other hand, $\underline{\varepsilon}(bv) \neq 0_S$ (since $0_S \notin \underline{\varepsilon}(N)$), and therefore $\underline{\varepsilon}(bv) \in R_3$, $(a, \underline{\varepsilon}(bv)) \in \alpha_3 = (R_3 \times R_3) \cup \mathrm{id}_R$ and, finally, $(ab, \underline{\varepsilon}(bv)b) = (o_S, \underline{\varepsilon}(bv)b) \notin \alpha_3$. We see that α_3 is not a congruence of R_S and, since $\alpha_3 \subseteq \alpha$, we come to the equality $\alpha = \alpha_2$. But this is a contradiction with $ab = o_S$ and 5.2.

We have proved that $o_S \notin R_2S_2$. Now, according to 6.6(2), the set K has at least one minimal element. If $\overline{a}, \overline{b} \in R_2$ are such that $\overline{a} + \overline{b} = o_S$ then $\overline{a}, \overline{b} \in R_3$, $(\overline{a}, \overline{b}) \in \alpha$ and $(\overline{a}, o_S) = (\overline{a} + \overline{a}, \overline{a} + \overline{b}) \in \alpha$, a contradiction. Thus $o_S \notin R_2 + R_2$ and. using 6.3(ii), we conclude that the set K has the smallest element, a contradiction with 3.19. □

6.9 Remark. Assume that $|R| = 2$. Then $|M| = 3$, $2 \leq |S| \leq 3$ and both S_1 and S_2 are subsemirings of S. In fact, if $|S| = 2$ then $S = R$ is simple, but the condition (f1) is not true. If $|S| = 3$ then $S = \{0_S, 1_S, o_S\}$ is not simple.

6.10 Theorem. The semiring S is simple if and only if the following three conditions are satisfied:

1. $S = R + S$.
2. $S_2 = S \setminus \{o_S\}$ is not a subsemiring of S.
3. If $0_S \in S$ then $S_1 = S \setminus \{0_S\}$ is not a subsemiring of S.

Proof. (i) Let S be simple. Then $S = R + S$ follows from 2.7. The right semimodule R_S is simple and faithful. Consequently, $|R| \geq 3$ anyway and $\alpha_2 \neq \mathrm{id}_R, R \times R$ ($\alpha_1 \neq \mathrm{id}_R, R \times R$ provided that $0_S \in S$). By 5.2 and 5.1, neither S_2 nor S_1 is a subsemiring of S.
(ii) Let the conditions (1), (2) and (3) be fulfilled. It follows from (1) and (2) thar either $a + b = o_S$ for some $a, b \in R_2$ or $cd = o_S$ for some $c \in R_2$ and $d \in S_2$. From (1) and (3) follows that if $0_S \in S$ then $ef = 0_S$ for some $e \in R_1$ and $f \in S_1$ (see 5.2 and 5.1). If the set K has no minimal element then $R_2 + R_2 = R_2$ by 6.3(i), and hence $cd = o_S$ and we use either 6.6 or 6.7 or 6.8 to show that S is simple. On the other hand, if the set K has a minimal element then the condition 6.6(2) is satisfied and we use 6.6, 6.7 or 6.8. □

7. Constructions

Let M $(= M(+))$ be a semilattice containing at least three elements and such that $0_M \in M$ and $o_M \in M$. The set $\underline{E}$ $(= \underline{E}_{0,1})$ of all endomorphisms f of M such that $f(0_M) = 0_M$ amd $f(o_M) = o_M$ is a unitary subsemiring of the full endomorphism semiring of M. The set $(\underline{D}_{0,1} =)\underline{D} = \{ f \in \underline{E} \,|\, |f(M)| \leq 2 \}$ $(= \{ f \in \underline{E} \,|\, f(M) = \{0_M, o_M\} \})$ is an ideal of the semiring $\underline{E}$ and there is a one-to-one correspondence between endomorphisms $q \in \underline{D}$ and prime ideals of the semilattice M; namely, $q \leftrightarrow A_q = \{ x \in M \,|\, q(x) = o_M \}$. If $f \in \underline{E}$ then $A_{qf} = \{ x \in M \,|\, f(x) \in A_q \}$ and $fq = q$. Consequently, $\underline{D} = \underline{R}(\underline{E})$ and, in fact, if E is a subsemiring of $\underline{E}$ such that $\underline{D} \subseteq E$ then $\underline{R}(E) = \underline{D}$.

For $x \in N = M \setminus \{o_M\}$ define $q_x \in \underline{D}$ by $q_x(y) = 0_M$ for $y \leq x$ and $q_x(z) = o_M$ for $z \not\leq x$. Then $A_q = \{ z \in M \,|\, z \not\leq x \}$ and the endomorphisms q_x correspond to principal prime ideals of the semilattice M. We put $(\underline{B}_{0,1} =)$ $\underline{B} = \{ q_x \,|\, x \in N \}$ and $(\underline{C}_{0,1} =)$ $\underline{C} = \{ q_{x_1} + \cdots + q_{x_n} \,|\, n \geq 1, x_i \in N \}$. Clearly, $\underline{C}$ is just the subsemiring of $\underline{D}$ generated by the set $\underline{B}$. The following three lemmas are obvious:

7.1 Lemma. *$\underline{C} = \underline{B}$ iff the ordered set $M(\leq)$ is a lattice.* □

7.2 Lemma. *$\underline{D} = \underline{B}$ iff $o_A \in A$ for every (proper) subsemilattice A of M.* □

7.3 Lemma. *Assume that every infinite strictly increasing sequence of element from M is upwards cofinal in N. Then $\underline{D} = \underline{B}$ iff either $o_N \in N$ or $N + N \neq N$.* □

In the remaining part of this section, let E be a subsemiring of $\underline{E}$ such that $\underline{B} \subseteq E$. The following three lemmas are obvious.

7.4 Lemma. (i) $\underline{C} \subseteq E$.
(ii) $\underline{R}(E) = E \cap \underline{D}$.
(iii) $q_{0_M} = o_E \in \underline{R}(E)$. □

7.5 Lemma. (i) *If $0_E \in E$ then $0_E \in \underline{R}(E)$ and $N + N = N$.*
(ii) *If $x \in N$ then $q_x = 0_E$ iff $x = o_N \in N$.*
(iii) *If $N + N = N$ then the mapping ξ, where $\xi(N) = \{0_M\}$ and $\xi(o_M) = o_M$, belongs to $\underline{D}$. If $o_N \in N$ then $\xi = q_{o_N} \in \underline{B}$.*
(iv) *If $N + N = N$ and $\xi \in E$ then $\xi = 0_E$.* □

7.6 Lemma. *Assume that every infinite strictly increasing sequence of elements from M is upwards cofinal in N. Then:*
(i) If $N + N \neq N$ then $o_N \notin N$, $0_E \notin E$ and $\underline{R}(E) = \underline{B} = \underline{D}$.
(ii) If $o_N \in N$ then $o_N \in N$, $0_E = q_{o_N}$ and $\underline{R}(E) = \underline{B} = \underline{D}$.
(iii) If $N + N = N$ and $o_N \notin N$ then $\xi \in \underline{D}$ (see 7.5(iii)) and $0_E \in E$ iff $\xi \in E$ (then $0_E = \xi$).
(iv) If $N + N = N$, $o_N \notin N$ and $\xi \in E$ then $\xi \notin \underline{B}$ and $\underline{R}(E) = \underline{D} = \underline{B} \cup \{\xi\}$.
(v) If $N + N = N$, $o_N \notin N$ and $\xi \notin E$ then $\xi \notin \underline{B} = \underline{R}(E)$ and $\underline{D} = \underline{B} \cup \{\xi\}$. □

The semilattice M becomes a left E-semimodule via the natural action of endomorphisms and we see readily that the conditions 3(a),...,(e) are fulfilled. In our case, $\underline{\varepsilon}(x) = q_x$, $x \in M \setminus \{o_M\}$ and ${}_EM$ is a characteristic semimodule.

In what follows, we restrict ourselves to the case when every infinite strictly increasing (decreasing, resp.) sequence of elements from M is upwards (downwards, resp.) cofinal in $N = M \setminus \{o_M\}$ ($L = M \setminus \{0_M\}$, resp.). This means that the conditions 6(g1) and 6(g2) are fulfilled. We still have to introduce two additional conditions.

(F1) For all $x \in N$ and $y, z \in K = M \setminus \{0_M, o_M\}$, $x < y$, there is at least one $f \in E$ such that $f(z) \leq y$ and $f(z) \not\leq x$.

(F2) For all $x, y \in K$ there is at least one $f \in E$ such that $f(x) = y$.

Notice that (F2) implies (F1) and if (F2) is true then $\{0_M\}$, $\{o_M\}$, $\{0_M, o_M\}$ and M are all (pair-wise different) subsemimodules of ${}_EM$.

7.7 Assume that $N + N \neq N$ (i.e., $o_M \in N + N$). Using (g1), we see that there is no infinite strictly increasing sequence of elements in M. By 7.6, the set N has at least two maximal elements, $0_E \notin E$ and $\underline{R}(E) = \underline{B}$ ($= \underline{D}$). The ordered set $M(\leq)$ is a lattice. Besides, (F1) is equivalent to 3(f1).

7.7.1 Theorem. *Assume that the set L (or K) has at least one minimal element. Then:*
(i) *There is no infinite strictly decreasing sequence of elements in M.*
(ii) *If* (F1) *is true then the semiring E is simple if and only if the set $\underline{B}$ is downwards cofinal in E (i.e., $E \subseteq \underline{E} + \underline{B}$).*

Proof. (i) This follows from (g2).
(ii) Since $N + N \neq N$, we have $|M| \geq 4$. Now, (F1) implies (f1) and it remains to use 6.6. □

7.7.2 Theorem. Assume that the set L has no minimal element and (F1) is true. The following conditions are equivalent:

(i) The semiring E is simple.

(ii) $\underline{B}$ is downwards cofinal in E (i.e., $E \subseteq \underline{E} + \underline{B}$) and there are $w \in K$ and $f \in E$ such that $f(K) \neq \{o_M\}$ and $f(x) \not\leq w$ for every $x \in K$.

(iii) $\underline{B}$ is downwards cofinal in E and there are $f, g \in E$ such that $f(K) \neq \{o_M\} \neq g(K)$ and $fg(K) = \{o_M\}$.

Proof. (i) implies (ii). We use 6.6. By 6.6(1), $E = E + \underline{B}$ and we take into account 6.6(2), where $o_E = q_{0_M}$.
(ii) implies (iii). We have $q_w f = q_{0_M} = o_E$, $q_w \neq o_E \neq f$.
(iii) implies (i). Use 6.6 again. □

7.8 Assume that $o_N \in N$. Then $N + N = N$, there is no infinite strictly increasing sequence of elements in M, $M(\leq)$ is a lattice, $0_E = q_{o_N} \in E$ and $\underline{R}(E) = \underline{B} = \underline{D}$ (see 7.1 and 7.6). Clearly, (F1) is equivalent to 3(f1).

7.8.1 Theorem. *Assume that the set L (or K) has at least one minimal element. Then:*
(i) *There is no infinite strictly decreasing sequence of elements in M.*
(ii) *If (F1) is true then the semiring E is simple.*

Proof. Use 6.7. □

7.8.2 Theorem. *Assume that the set L has no minimal element and (F1) is true. The following conditions are equivalent:*

(i) *The semiring E is simple.*

(ii) *There are $w \in K$ and $f \in E$ such that $f(K) \neq \{o_M\}$ and $f(x) \not\leq w$ for every $x \in K$.*

(iii) *There are $f, g \in E$ such that $f(K) \neq \{o_M\} \neq g(K)$ and $fg(K) = \{o_M\}$.*

Proof. Use 6.7. □

7.9 Assume that $o_N \notin N$, $N + N = N$ (then N has no maximal element) and $\xi \in E$ (by 7.6(iii), we have $\xi \in E$ iff $0_E \in E$, and then $0_E = \xi$). By 7.6(iv), $\underline{R}(E) = \underline{D} = \underline{B} \cup \{\xi\}$ and $\xi = 0_E \notin \underline{B}$. Now, (F1) is equivalent to 3(f1) (use the fact that $o_N \notin N = N + N$).

7.9.1 Theorem. *Assume that the set L (or K) has at least one minimal element. Then:*
(i) *There is no infinite strictly decreasing sequence of elements in M.*
(ii) *If (F1) is true then the semiring E is simple if and only if the following two equivalent conditions are satisfied:*

(ii1) *There are $w \in K$ and $f \in E$ such that $\{0_M\} \neq f(K) \leq w$.*

(ii2) *There are $f, g \in E$ such that $f(K) \neq \{0_M\} \neq g(K)$ and $fg(K) = \{0_M\}$.*

Proof. Use 6.8. □

7.9.2 Theorem. *Assume that the set L has no minimal element and (F1) is true. The following conditions are equivalent:*

(i) *The semiring E is simple.*

(ii) *There are $w_1, w_2 \in K$ and $f_1, f_2 \in E$ such that $f_1(K) \neq \{o_M\}$, $f_2(K) \neq \{0_M\}$, $f_1(K) \not\leq w_1$ and $f_2(K) \leq w_2$ for every $x \in K$.*

(iii) *There are* $f_1, f_2, g_1, g_2 \in E$ *such that* $f_1(K) \neq \{o_M\} \neq g_1(K)$, $f_2(K) \neq \{0_M\} \neq g_2(K)$, $f_1g_1(K) = \{o_M\}$ *and* $f_2g_2(K) = \{0_M\}$

Proof. Use 6.8. □

7.10 Assume that $o_N \notin N$, $N + N = N$ (then N has no maximal element) and $\xi \notin E$. Then $0_E \notin E$ by 7.6(iii) and, by 7.6(v), $\underline{R}(E) = \underline{B}$. Now, (F1) is equivalent to 3(f1).

7.10.1 Theorem. *Assume that the set* L *(or* K*) has at least one minimal element. Then:*
(i) *There is no infinite strictly decreasing sequence of elements in* M.
(ii) *If (F1) is true then the semiring* E *is simple if and only if* $E \subseteq \underline{E} + \underline{B}$.

Proof. Use 6.6. □

7.10.2 Theorem. *Assume that the set* L *has no minimal element and (F1) is true. The following conditions are equivalent:*

(i) *The semiring* E *is simple.*

(ii) $E \subseteq \underline{E} + \underline{B}$ *and there are* $w \in K$ *and* $f \in E$ *such that* $f(K) \neq \{o_M\}$ *and* $f(x) \not\leq w$ *for every* $x \in K$.

(iii) $E \subseteq \underline{E} + \underline{B}$ *and there are* $f, g \in E$ *such that* $f(K) \neq \{o_M\} \neq g(K)$ *and* $fg(K) = \{o_M\}$.

Proof. Use 6.6. □

7.11 Remark. (cf. 3.22) (i) Assume that there is an endomorphism $f \in E$ such that $f(M)$ is finite, $f(N) \subseteq N$ and $|f(M)| \geq 3$.

We have $f(M) = \{0_M, w_1, \ldots, w_n, o_M\}$, $n \geq 1$, $w_i \in K$. Assume that $w = w_1 + \cdots + w_n \in K$ (e.g., $n = 1$ or $N + N = N$) and $w \neq o_N$. Then $q_w f(N) \subseteq q_w(\{0_M, w_1, \ldots, w_n\}) = \{0_M\}$. Consequently, $q_w f = \xi = 0_E \in E$. If $o_N \in N$ then $q_w f = q_{o_N} = 0_E$. Of course, since $w \neq o_N$, we have $q_w \neq 0_E$. Since $f \notin \underline{R}(E)$, we have $f \neq 0_E$ as well.
(ii) Assume that $N + N = N$ and let $u, v \in K$ be such that $u < v$. Put $f(K) = \{u\}$, $g(K) = \{v\}$, $f(0_M) = 0_M = g(0_M)$ and $f(o_M) = o_M = g(o_M)$. Clearly, $f, g \in \underline{E}$, $f(M) = \{0_M, u, o_M\}$, $g(M) = \{0_M, v, o_M\}$, $f(N) = \{0_M, u\}$, $g(N) = \{0_M, v\}$, $q_u f = \xi$, $f \neq \xi \neq q_u$, $q_u g = q_{0_M}$ and $q_u \neq q_{0_M} \neq g$.

References

[1] R. El Bashir, J. Hurt, A. Jančařík and T. Kepka, *Simple commutative semirings,* J. Algebra, 263 (2001), 277-306.

[2] R. El Bashir and T. Kepka, *Congruence-simple semirings,* Semigroup Forum, 75 (2007), 588-608.

[3] V. Flaška, *One very particular example of a congruence-simple semiring,* Europ. J. Comb., 30 (2009), 759-763.

[4] J. Golan, *The Theory of Semirings with Applications in Mathematics and Theoretical Computer Science,* Pitman Monographs, 54, Longman, Harlow, 1992.

[5] V. Hebisch and H. J. Weinert, *Halbringe - Algebraische Theorie und Anwendungen in der Informatik,* Teubner, Stuttgart, 1993.

[6] J. Ježek and T. Kepka, *The semiring of 1-preserving endomorphisms of a semilattice,* Czech. Math. J., 59 (2009), 999-1003.

[7] J. Ježek, T. Kepka and M. Maróti, *The endomorphism semiring of a semilattice,* Semigroup Forum, 78 (2009), 21-26.

[8] A. Kendziorra, J. Zumbrägel, *Finite simple additively idempotent semirings,* J. Algebra, 388 (2013), 43-64.

[9] G. Maze, C. Monico and J. Rosenthal, *Public key cryptography based on semigroup actions,* Adv. Math. Commun., 1 (2007), 489-507.

[10] S. S. Mitchell and P. B. Fenoglio, *Congruence-free commutative semirings,* Semigroup Forum, 37 (1988), 79-91.

[11] C. Monico, *On finite congruence-simple semirings,* J. Algebra, 271 (2004), 846-854.

[12] J. Zumbrägel, *Classification of finite congruence-simple semirings with zero,* J. Algebra Appl., 7 (2008), 363-377.

Accepted: 3.05.2018