Minimal left ideals in 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. Minimal left ideals in semirings are investigated.
Keywords: semiring, semimodule, semilattice, ideal, endomorphism.

Simple semirings appear in many fields of mathematics. In order to characterize simple semirings with bi-absorbing element, it is necessary to have some information on minimal left ideals. In this note, basic properties of minimal left ideals in semirings are investigated.

1. Prerequisitities

1.1 Semigroups. Let $S = S(*)$ be a semigroup. If A, B are subsets of S then $A * B = \{ a * b \,|\, a \in A, b \in B \}$. An element $a \in S$ is called *left/right neutral* (*absorbing*) if $a * b = b$ / $b * b = b$ ($a * b = a$ / $b * a = a$) for every $b \in S$. We denote by $\underline{L}(S(*))$ ($\underline{R}(S(*))$) the set of left (right) absorbing elements and we put $\underline{L}^+(S(*)) = \{ a \in S \,|\, |a * S| = 1 \}$ ($\underline{R}^+(S(*)) = \{ a \in S \,|\, |S * a| = 1 \}$).

The semigroup S is called

- *left* (*right*) *cancellative* if $a * b \neq a * c$ ($b * a \neq c * a$) for all $a, b, c \in S$, $b \neq c$,
- *idempotent* if $a * a = a$ for every $a \in S$,

*. Corresponding author

- *constant* if $|S * S| = 1$.

If the semigroup S is commutative then, for $a, b \in S$, we write $a \leq b$ iff $b \in (a * S) \cup \{a\}$. We write $a < b$ iff $a \leq b|$ and $a \neq b$.

1.2 Semirings. A *semiring* is an algebraic structure with two associative binary operations, usually denoted as addition and multiplication, where the addition is commutative and the multiplication distributes over the addition.

Let S be a semiring. Then $0_S \in S$ ($o_S \in S$) means that S has the uniquely determined additively neutral (absorbing) element 0_S (o_S). On the other hand, $0_S \notin S$ ($o_S \notin S$) means that no such element exists in S. Similarly, $1_S \in S$ means that S contains the uniquely determined multiplicatively neutral element 1_S. There is no specific way how to denote multiplicatively absorbing elements, but if the additively neutral element 0_S is multiplicatively absorbing then 0_S is called the *zero* element. The set of left (right) multiplicatively absorbing elements will be denoted by $\underline{L}(S)$ ($\underline{R}(S)$) in the sequel.

The semiring S is called *congruence-simple* if it has just two congruence relations. The following basic classification of congruence-simple semirings can be found in [1], Theorem 2.1 and Lemma 1.4.

Proposition 1.2.1. *Let S be a congruence-simple semiring. Then just one of the following four cases takes place:*

1. *S is additively cancellative;*
2. *S is additively idempotent;*
3. *S is additively constant;*
4. *$o_S \in S$, $2S = \{o_S\}$ and $S + S = S$ (and S is infinite).*

Every two-element semiring is congruence-simple and there are just ten two-element semirings up to isomorphism:

$S_1(+)$	0	a
0	0	a
a	a	0

$S_1(\cdot)$	0	a
0	0	0
a	0	a

$S_2(+)$	0	a
0	0	a
a	a	0

$S_2(\cdot)$	0	a
0	0	0
a	0	0

$S_3(+)$	0	o
0	0	o
o	o	o

$S_3(\cdot)$	0	o
0	0	0
o	0	0

$S_4(+)$	0	o
0	0	o
o	o	o

$S_4(\cdot)$	0	o
0	o	o
o	o	o

$S_5(+)$	0	o
0	0	o
o	o	o

$S_5(\cdot)$	0	o
0	0	0
o	0	o

$S_6(+)$	0	o
0	0	o
o	o	o

$S_6(\cdot)$	0	o
0	0	o
o	o	o

$S_7(+)$	0	o
0	0	o
o	o	o

$S_7(\cdot)$	0	o
0	0	0
o	o	o

$S_8(+)$	0	o
0	0	o
o	o	o

$S_8(\cdot)$	0	o
0	0	o
o	0	o

$S_9(+)$	a	o
a	o	o
o	o	o

$S_9(\cdot)$	a	o
a	o	o
o	o	o

$S_{10}(+)$	a	o
a	o	o
o	o	o

$S_{10}(\cdot)$	a	o
a	a	o
o	o	o

1.3 Semimodules. Let S be a semiring. A (*left* $S-$) *semimodule* is a commutative semigroup M $(= M(+))$ together with a scalar multiplication $S \times M \to M$. The semimodule M is called

- *minimal* if $|M| \geq 2$ and $N = M$ whenever N is a non-trivial subsemimodule of M;
- *simple* if it has just two congruence relations;
- *faithful* if for all $a, b \in S$, $a \neq b$, there is at least one $x \in M$ with $ax \neq bx$.

2. Ideals-basic facts

Let S be a non-trivial semiring. A non-empty subset I of S is called

- a *left* (*right*) *ideal* if $(I + I) \cup SI \subseteq I$ $((I + I) \cup IS \subseteq I)$;
- an *ideal* if $(I + I) \cup SI \cup IS \subseteq I$;
- a *bi-ideal* if $(S + I) \cup SI \cup IS \subseteq I$.

A (left, right, bi-) ideal is said to be

- *trivial* if $|I| = 1$;
- *proper* if $I \neq S$;
- *minimal* if it is non-trivial and $K = I$ whenever K is a non-trivial (left, right, bi-) ideal such that $K \subseteq I$.

The semiring S is called

- *(left, right, bi-) ideal-simple* if S has no proper non-trivial (left, right, bi-) ideal;
- (*left, right, bi-*) *ideal-free* if S has no proper (left, right, bi-) ideal.

The following four assertions are straightforward.

Lemma 2.1. *Let $a \in S$. Then:*

(i) *The one-element set $\{a\}$ is a left (right) ideal of S iff the element a is right (left) multiplicatively absorbing.*

(ii) *The set $\{a\}$ is a bi-ideal iff a is bi-absorbing.* □

Lemma 2.2. *Assume that $\underline{L}(S) \neq \emptyset$ ($\underline{R}(S) \neq \emptyset$). Then:*

(i) *$\underline{L}(S)$ ($\underline{R}(S)$) is an ideal and it is the smallest left (right) ideal of S.*

(ii) *$|\underline{L}(S)| = 1$ iff $|\underline{R}(S)| = 1$ and then $\underline{L}(S) = \{a\} = \underline{R}(S)$, where a is multiplicatively absorbing.*

(iii) *If $|\underline{L}(S)| \geq 2$ ($|\underline{R}(S)| \geq 2$) then $\underline{R}(S) = \emptyset$ ($\underline{L}(S) = \emptyset$).*

(iv) *$\underline{L}(S)$ ($\underline{R}(S)$) is bi-idempotent.*

(v) *If $a, b \in \underline{L}(S)$ ($a, b \in \underline{R}(S)$) are such that $a < b$ then the two-element set $\{a, b\}$ is a minimal right (left) ideal.* □

Lemma 2.3. (i) *$\underline{L}(S) \subseteq \underline{L}^+(S)$ ($\underline{R}(S) \subseteq \underline{R}^+(S)$) and $\underline{L}^+(S)$ ($\underline{R}^+(S)$) is an ideal of S, provided that $\underline{L}^+(S) \neq \emptyset$ ($\underline{R}^+(S) \neq \emptyset$).*

(ii) *There is a mapping $\alpha : \underline{L}^+(S) \to \underline{L}(S)$ ($\alpha : \underline{R}^+(S) \to \underline{R}(S)$) such that $aS = \{\alpha(a)\}$ ($Sa = \{\alpha(a)\}$) for every $a \in \underline{L}^+(S)$ ($a \in \underline{R}^+(S)$).*

(iii) *$\alpha \,|\, \underline{L}(S) = \mathrm{id}$ ($\alpha \,|\, \underline{R}(S) = \mathrm{id}$).*

(iv) *$\alpha^2 = \alpha$, $\alpha(a + b) = \alpha(a) + \alpha(b)$ and $\alpha(ca) = c\alpha(a)$ ($\alpha(ac) = \alpha(a)c$) for all $a, b \in \underline{L}^+(S)$ ($a, b \in \underline{R}^+(S)$) and $c \in S$.* □

Lemma 2.4. *If I is a bi-ideal of S then the relation $(I \times I) \cup \mathrm{id}_S$ is a congruence of the semiring S. In particular, the semiring S is bi-ideal-simple, provided that it is congruence-simple.* □

3. Minimal left ideals-basic observations (a)

In this part, let S be a semiring and K be a minimal left ideal of S. We put $A = \{\, a \in K \mid Sa = K \,\}$, $B = K \cap \underline{R}^+(S) = \{\, a \in K \mid |Sa| = 1 \,\}$, $C = K \cap \underline{R}(S) = \{\, a \in K \mid Sa = \{a\} \,\}$, $D = \{\, a \in K \mid Ka = K \,\}$, $E = \{\, a \in K \mid |Ka| = 1 \,\}$ and $F = \{\, a \in K \mid Ka = \{a\} \,\}$.

The following seven assertions are easy.

Lemma 3.1. (i) *$A \cup B = K$ and $A \cap B = \emptyset$.*

(ii) *B is a left ideal of S, provided that $B \neq \emptyset$.*

(iii) *Either $B = \emptyset$ or $|B| = 1$ or $B = K$.*

(iv) *$C \subseteq B$, $\underline{R}(S)K \subseteq C$ and $C \neq \emptyset$ iff $\underline{R}(S) \neq \emptyset$.*

(v) *$D \cup E = K$ and $D \cap E = \emptyset$.*

(vi) *$D \subseteq A$, $B \subseteq E$ and $C \subseteq F \subseteq E$.*

(vii) *If $E \neq \emptyset$ then E is an ideal of K.* □

Lemma 3.2. *Let $B = K$* (see 3.1(iii))*. Then just one of the following five cases holds:*

1. $K \subseteq \underline{R}(S)$, $|K| = 2$ *and* $K = \{0_K, o_K\}$;
2. $SK = \{0_K\}$ *and* $K = \{0_K, o_K\}$;
3. $SK = \{o_K\}$ *and* $K = \{0_K, o_K\}$;
4. $SK = \{o_K\} = K + K$ *and* $|K| = 2$;
5. $SK = \{0_K\}$ *and* $K(+)$ *is a finite cyclic group of prime order.* □

Lemma 3.3. *Let* $B = K$ *and* $|K| \geq 3$. *Then* $SK = \{0_K\}$ *and* $K(+)$ *is a finite cyclic group of prime odd order.* □

Lemma 3.4. *Let* $|B| = 1$ (see 3.1(iii)). *Then just one of the following two cases holds:*

1. $B = \{0_K\}$, $0_K K = \{0_K\} = S0_K$ *and* $Sa = K$ *for every* $a \in K \setminus \{0_K\}$. *Besides, either* $0_K S \subseteq \underline{R}(S)$ *and* $|0_K S| \geq 2$ *or* 0_K *is multiplicatively absorbing in* S, $K \subseteq S + 0_K$ *and* $S + 0_K$ *is a bi-ideal of* S;
2. $B = \{o_K\}$, $o_K K = \{o_K\} = So_K$ *and* $Sa = K$ *for every* $a \in K \setminus \{o_K\}$. *Besides, either* $o_K S \subseteq \underline{R}(S)$ *and* $|o_K S| \geq 2$, *or* o_K *is multiplicatively absorbing in* S, $K \cap (S + o_K) = \{o_K\}$ *and* $S + o_K$ *is a bi-ideal of* S. □

Lemma 3.5. *Let* $B = \{0_K\}$ (see 3.4). *Then:*
(i) $E = \{\, a \in K \mid Ka = \{0_K\}\,\}$.
(ii) $0_K \in L = \{\, a \in S \mid aK = \{0_K\}\,\}$ *and* L *is an ideal of* S.
(iii) *If* $K \subseteq L$ *then* $KK = \{0_K\}$, $E = K$ *and* $K \times K = \varrho$, *where* ϱ *is the congruence of* S *defined by* $(a, b) \in \varrho$ *iff* $ac = bc$ *for every* $c \in K$.
(iv) *If* $K \nsubseteq L$ *then* $LK = K \cap L = \{0_K\}$. □

Lemma 3.6. *Let* $B = \{o_K\}$ (see 3.4). *Then:*
(i) $E = \{\, a \in K \mid Ka = \{o_K\}\,\}$.
(ii) $o_K \in L = \{\, a \in S \,|aK = \{o_K\}\,\}$ *and* L *is an ideal of* S.
(iii) *If* $K \subseteq L$ *then* $KK = \{o_K\}$, $E = K$ *and* $K \times K \subseteq \varrho$ (see 3.5(iii).
(iv) *If* $K \nsubseteq L$ *then* $LK = K \cap L = \{o_K\}$. □

Lemma 3.7. *Let* $B = \{0_K\}$ see 3.4) *and* $J = \{\, a \in K \mid 0_K \in K + a\,\}$. *Then:*
(i) J *is a left ideal of* S.
(ii) *Either* $J = \{0_K\}$ *or* $J = K$.
(iii) *If* $J = \{0_K\}$ *then* $K + (K \setminus \{0_K\}) \subseteq K \setminus \{0_K\}$.
(iv) *If* $J = K$ *then* $K(+)$ *is a group.* □

Lemma 3.8. *Let* $B = \{0_K\} = J$ (see 3.7). *Then either* $E = K$ *or* D *is a subsemiring of* K *(in fact,* $K + D \subseteq D$*).*

Proof. Assume that $D \neq \emptyset$. Clearly, $DD \subseteq D$. If $a, b \in K$ are such that $a + b \notin D$ then $a + b \in E$, $K(a + b) = \{0_K\}$ by 3.5(i), and hence $ca + ab = 0_K$ for every $c \in K$. Now, $ca = 0_K = cb$ follows from 3.7(iii), so that $a, b \in E$. □

Lemma 3.9. *$Da = D$ for every $a \in D$.*

Proof. Clearly, $DD \subseteq D$. If $a, b \in D$ then $b = ca$ for some $c \in K$ and $K = Kb = Kca$, $|Kc| \geq 2$ and $c \in D$. □

Lemma 3.10. *Assume that K is multiplicatively idempotent. Then just one of the following three cases is true:*

1. *K is additively idempotent and $ab = a$ for all $a, b \in K$ (then $E = \emptyset$);*
2. *$|K| = 2$ and $K \cong S_8$ (then $E = K$);*
3. *$|E| = 1$.*

Proof. We have $Ka = \{a^2\} = \{a\}$ for every $a \in E$, and hence $E \subseteq \underline{R}(S)$ and $E = \underline{R}(S) \cap K$. If $|E| \geq 2$ then $K \subseteq \underline{R}(S)$ and it is clear that $K \cong S_8$. On the other hand, if $E = \emptyset$ then $Ka = K$ and $baa = ba$ for all $a, b \in K$. Thus $ab = a$ for all $a, b \in K$. □

4. Minimal left ideals-basic observations (b)

Let S be a semiring and K be a minimal left ideal such that $|B| = 1$ (see 3.4). Then $B = \{q\}$, where either $q = 0_K$ or $q = o_K$. Besides, $q \in \underline{R}(S)$, $K\underline{R}(S) = K \cap \underline{R}(S) = \{q\}$, $qS \subseteq \underline{R}(S)$ and $qK = \{q\}$, so that q is multiplicatively absorbing in K. We have $Sa = K$ for every $a \in K \setminus \{q\}$, $KE = \{q\}$, E is an ideal of K and $Ka = K$ for every $a \in D = K \setminus E$ (see 3.5, 3.6).

Lemma 4.1. (i) *$q \notin (K \setminus \{q\})a$ for every $a \in D$.*

(ii) *If $a \in K$ then either $Ba \neq b$ for every $b \in K$, $b \neq q$, or a is right multiplicatively neutral in K.*

Proof. (i) The set $\{\, b \in S \mid ba = q \,\}$ is a left ideal of S.

(ii) The set $\{\, b \in K \mid ba = b \,\}$ is a left ideal of S. □

The following six assertions are straightforward.

Lemma 4.2. *Let $a \in K$ be such that $a^2 = a$. Then:*

(i) *If $a \neq q$ then a is right multiplicatively neutral in K.*

(ii) *If $a \neq q$ then $(a + q)^2 = a + b + ab + b^2$ for every $b \in K$. If, moreover, $b^2 = b \neq q$ then $(a + b)^2 = 2(a + b)$.*

(iii) *$(a + q)^2 = a + q$.*

(iv) *If $a \neq q$ then $(ba)^2 = b^2$ for every $b \in K$.*

(v) *If* $a \neq q$ *then* $(ab)^2 = ab^2$ *for every* $b \in K$.

(vi) *If* $b \in K$ *is such that* $b^2 = b \neq q$ *then* $2c = c(a+b)$ *for every* $c \in K$. *If, moreover,* $2c \neq q$ *then* $a + b \neq q$. *If* $2c = c \neq q$ *then* $(a+b)^2 = a + b$. □

Put $I_a(K) = \{\, a \in K \mid 2a = a \,\}$, $I_m(K) = \{\, a \in K \mid a^2 = a \,\}$ and $I_z(K) = \{\, a \in K \mid 2a = q \,\}$.

Lemma 4.3. (i) $q \in I_a(K)$ *and* $I_a(K)$ *is a left ideal of* S.

(ii) *Either* $I_a(K) = \{q\}$ *or* $I_a(K) = K$ *(so that* K *is additively idempotent).* □

Lemma 4.4. (i) $q \in I_z(K)$ *and* $I_z(K)$ *is a left ideal of* S.

(ii) *Either* $I_z(K) = \{q\}$ *or* $I_z(K) = K$.

(iii) *If* $I_z(K) = K$ *then* $I_a(K) = \{q\}$.

(iv) *If* $I_z(K) = \{q\} = I_a(K)$ *and either* $q = o_K$, *or* $q = 0_K$ *and* $J = \{0_K\}$ (see 3.7(iii)) *then, for every* $a \in K \setminus \{q\}$, *the additive subsemigroup* $\mathbb{N}a = \{a, 2a, 3a, \dots\}$ *is a copy of the additive semigroup of positive integers.* □

Lemma 4.5. *Let* $I_a(K) = K$. *Then:*

(i) $I_m(K)$ *is a subsemiring of* K.

(ii) $q \in I_m(K)$ *and* $ab = a$ *for all* $a, b \in I_m(K)$, $b \neq q$.

(iii) *If* $a \in I_m(K) \setminus \{q\}$ *then* a *is right multiplicatively neutral in* K.

(iv) $a + b \neq q$ *for all* $a, b \in I_m(K) \setminus \{q\}$. □

Lemma 4.6. *Let* $a \in K$ *be such that* $a^m = a$ *for some* $m \geq 2$. *Put* $b = a + a^2 + \cdots + a^{m-1}$. *Then:*

(i) $ab = b = ba$.

(ii) *If* $b = q = 0_K$ *and* $a \neq 0_K$ *then* $K(+)$ *is a p-elementary group for a prime* p (see 3.7).

(iii) *If* $b \neq q$ *then* a *is right multiplicatively neutral in* K, $a \in I_m(K)$ *and* $b = ma$. □

Lemma 4.7. *Let* $a \in K$ *be such that* $q \neq a^m \in I_m(K)$. *Then* $a^{m+1} = a$. □

Lemma 4.8. *Let* $a \in K$ *and* $1 \leq m < n$ *be such that* $a^m = a^n$. *Then* $a^{m(n-m)} \in I_m(K)$.

Proof. As $a^n = a^m \cdot a^{n-m} = a^m$, we have $a^m = a^m \cdot a^{n-m} \cdot a^{n-m} = \cdots = a^m \cdot a^{m(n-m)}$, and hence $a^{m(n-m)} \cdot a^{m(n-m)} = a^{m(n-m)}$. □

Lemma 4.9. *Let* $a \in K \setminus I_m(K)$ *be such* $q \neq a + a^2 + \cdots + a^k$ *for every* $k \geq 1$. *Then either* $q = 0_K = a^l$ *for some* $l \geq 2$ *or the multiplicative subsemigroup* $a^{\mathbb{N}} = \{a, a^2, a^3, \dots\}$ *is a copy of the additive semigroup of positive integers.*

Proof. Assume, on the contrary, that $a^m = a^n$ for some $1 \leq m < n$. By 4.8, $a_1 = a^{m(n-m)} \in I_m(K)$. By 4.7, either $a^{m(n-m)+1} = a$ or $a^{m(n-m)} = q$. If $a^{m(n-m)} = a$ then $ab = b = ba$ for $b = a + a^2 + \cdots + a^{m(n-m)}$, $b \neq q$ and $a \in I_m(K)$ by 4.1(ii), a contradiction. Thus $a^{m(n-m)} = q$, and hence $q = 0_K$ (if $q = o_K$ then $a + a^2 + \cdots + a^{m(n-m)} = o_K = q$). □

Lemma 4.10. *Assume that* $q = 0_K$.

(i) *If* $a \in E$ *then* $a^{\mathbb{N}} = \{0_K, a\}$ *and* $\mathbb{N}a \cup \{0_K\}$ *is the subsemiring of* K *generated by* a.

(ii) *If* $a \in I_m(K)$ *then* $a^{\mathbb{N}} = \{a\}$ *and* $\mathbb{N}a$ *is the subsemiring of* K *generated by* a.

(iii) *If* K *is not a ring and* $a \in D \setminus I_m(K)$ *then* $a^{\mathbb{N}}$ *is a copy of the additive semigroup of positive integers,* $\langle a \rangle = \{\, \sum_{i=1}^{m} n_i a_i \mid m \geq 1, 0 \leq n_i, \sum n_i \neq 0 \,\}$ *is the subsemiring of* K *generated by the element* a *and* $\langle a \rangle \subseteq D$.

Proof. (i) We have $a^2 = 0_K$.

(ii) We have $a^2 = a$.

It follows from 4.1(i) that $0_K \notin a^{\mathbb{N}}$. We have $a \in D$ and D is a subsemiring of K by 3.8. Thus $\langle a \rangle \subseteq D$. The rest follows from 4.9. □

For $e \in I_m(K)$, let $G_e^+ = \{\, a \in K \mid ea = a \,\}$ and $G_e = G_e^+ \setminus \{q\}$.

Lemma 4.11. *Let* $e \in I_m(K)$. *Then* $e, q \in G_e^+$ *and* G_e^+ *is a right ideal of the semiring* K*, If* $e = q$ *then* $G_e^+ = \{q\}$. *If* $e \neq q$ *then* $|G_e^+| \geq 2$ *and* e *is multiplicatively neutral in* G_e^+. □

Lemma 4.12. *Let* $e \in I_m(K) \setminus \{q\}$. *Then* G_e *is a subgroup of the multiplicative semigroup* $K(\cdot)$ *and* e *is the multiplicatively neutral element of* G_l. *Moreover,* $G_l \subseteq D$.

Proof. Clearly, $e \in G_e$. If $a, b \in G_e$ then $a \in Ka$, $b \in Kb$, and hence $a, b \in D$, $ab \in D$ and $ab \in G_e$. By 4.5(iii), e is right multiplicatively neutral in K, so that e is the multiplicatively neutral element of G_e.

Let $a \in G_e$. Then $ba = e$ for some $b \in K$, $eb = bab$ and $a = ae = aba$. We have $ab \neq q$, and therefore $b \in D$ and $cb = e$ for some $c \in K$. Then $a = ea = cba = cb = c$, $ab = e$, $eb = be = b$ and we see that G_e is a multiplicative group. □

Lemma 4.13. *Let* $e, f \in I_m(K) \setminus \{q\}$, $e \neq f$. *Then* $G_e \cap G_f = \emptyset$.

Proof. If $a \in G_e \cap G_f$ then $ea = a = fa$. But $e = ab$ for some $b \in G_e$ and we have $f = fe = fab = ab = e$. □

Lemma 4.14. *Assume that no subsemigroup of the multiplicative semigroup of D is a copy of the additive semigroup of positive integers. Then $D = \bigcup G_e$, $e \in I_m(K) \setminus \{q\}$.*

Proof. Let $a \in D$. Then $ba = a$ for some $b \in D$ (see 3.9), and hence $b^m a = a$ for every $m \geq 1$. According to our assumption, $b^n \in I_m(K) \setminus \{q\}$ for some $n \geq 1$. □

Lemma 4.15. *Let $e, f \in I_m(K) \setminus \{q\}$. The mapping $a \mapsto fa$ is an isomorphism of the multiplicative group G_e onto the multiplicative group G_f.*

Proof. First, $ffa = fa$, and so $fa \in G_f$. Furthermore, by 4.5(iii), $fab = fafbF$ for all $a, b \in G_e$, and therefore $a \mapsto fa$ is a multiplicative homomorphism of G_e into G_f. If $a \in G_e$ is such that $fa = f$ then a is right multiplicatively neutral in K by 4.1(ii), and so $a = ea = e$. It means that the homomorphism is injective. Finally, if $c \in G_f$ then $ec \in G_e$ and $fewc = fc = c$. □

Lemma 4.16. *Assume that K is multiplicatively idempotent. Then $ab = a$ for all $a, b \in K$, $b \neq q$, and just one of the following three cases holds:*

1. *$|K| = 2$ and $K \cong S_1$ (then $q = 0_K$);*
2. *K is additively idempotent;*
3. *$q = o_K$ and $2a = o_K$ for every $a \in K.o$*

Proof. It follows immediately from 4.2(i) that $ab = a$ for all $a, b \in K$, $b \neq q$. Now, $c(a + b) = ca + cb = 2c$ for all $c \in K$ and $a, b \in K \setminus \{q\}$. If $a + b = q$ then $2c = q$ and $I_z(K) = K$. If, moreover $q = 0_K$ then $K(+)$ is a 2-elementary group and $a = a(a + b) = aa + ab = 2a = 0_K$ for $0_K \neq a \neq b \neq 0_K$. Now, it follows easily that $|K| = 2$ and $K \cong S_1$. Finally, if $a + b \neq q$ for all $a, b \in K \setminus \{q\}$ then $K(+)$ is idempotent. □

5. Partial summary (a)

Let S be a semiring and K be a minimal left ideal of S such that $B = \{0_K\}$ (see 3.4). We put $K^* = K \setminus \{0_K\}$ and $I_m(K)^* = I_m(K) \setminus \{0_K\}$.

Proposition 5.1. (i) $0_K K = \{0_K\} = S0_K$.

(ii) $0_K S \subseteq \underline{R}(S)$.

(iii) *$Sa = K$ for every $a \in K^*$.*

(iv) $0_K \in L = \{\, a \in S \mid aK = \{0_K\} \,\}$ *and L is an ideal of S.*

(v) *If $K \subseteq L$ then $KK = \{0_K\}$ and $K \times K \subseteq \varrho$, where ϱ is the congruence of S defined by $(a, b) \in \varrho$ iff $ac = bc$ for every $c \in K$.*

(vi) *If $K \subseteq L$ and $\varrho = S \times S$ then $SK = \{0_K\}$.*

(vii) *If* $SK = \{0_K\}$ *(or* $L = S$*) then either* $|K| = 2$ *or* $K(+)$ *is a finite (cyclic) group of prime order.* (viii) *If* $K \nsubseteq L$ *then* $LK = L \cap K = \{0_K\}$*.*

(ix) *If* $|\underline{R}(S)| = 1$ *then* 0_K *is multiplicatively absorbing in* S *and* $S + 0_K$ *is a bi-ideal of* S*.*

(x) *If* $S + 0_K = S$ *then* $0_K = 0_S$*.*

(xi) $E = \{ a \in K \mid |Ka| = 1 \} = \{ a \in K \mid Ka = \{0_K\} \}$*.*

(xii) $E = K$ *iff* $K \subseteq L$ (see (v) and (vi)).

(xiii) $DD = D = \{ a \in K \mid Ka = K \}$ *and* $Da = D$ *for every* $a \in D$*.*

(xiv) $K = E \cup D$ *and* $E \cap D = \emptyset$*.*

(xv) $0K \notin K^*D$*.*

(xvi) *Either* K *is additively idempotent or* $2a \neq a$ *for every* $a \in K^*$*.*

(xvii) *Either* $2a = 0_K$ *for every* $a \in K$ *(so that* $K(+)$ *is a 2-elementary group), or* $2b \neq 0_K$ *for every* $b \in K^*$ *and* $K = \{ 2a \mid a \in K \}$*.*

(xviii) *Either* $K(+)$ *is a group or* $K + K^* \subseteq K^*$*.*

(xix) *If* $a \in I_m(K)^*$ *then* a *is right multiplicatively neutral in* K*.*

(xx) $I_m(K)^* \subseteq D$*.*

Proof. See 3.4, 3.5, 3.7, 3.8, 3.9 and 4.2, 4.3, 4.4. □

Proposition 5.2. *Assume that* $K(+)$ *is not a group and that* $KK \neq \{0_K\}$*. Then:*

(i) $K + K^* \subseteq K^*$*.*

(ii) D *is a subsemiring of* K *and* $K + D \subseteq D$*.*

(iii) *For every* $e \in I_m(K)^*$, $G_e = eK^* = \{ a \in K \mid ea = a \}$ *is a subsemiring of* K*,* e *is the multiplicatively neutral element of* G_e *and the multiplicative semigroup of* G_e *is a group.*

(iv) $G_e^* = G_e \cup \{0_K\} = eK$ *is a right ideal of* K*.*

(v) *Either* $G_e = \{e\}$ *or the multiplicative group of* G_e *is infinite and torsion-free.*

(vi) *If* $e, f \in I_m(K)^*$*,* $e \neq f$*, then* $G_e \cap G_f = \emptyset$ *and the mapping* $G_e \to fG_e = G_f$ *is an isomorphism of the semiring* G_e *onto the semiring* G_f*.*

Proof. See 3.7(iii), 4.10, 4.11, 4.12, 4.13 and 4.15. □

Proposition 5.3. *Assume that* $K(+)$ *is not a group,* $KK \neq \{0_K\}$ *and no multiplicative subsemigroup of* D *is a copy of the additive semigroup of positive integers. Then:*

(i) $D = I_m(K)^*$ *is a subsemiring of* K*,* $K + D \subseteq D$ *and* D *is just the set of elements from* K *that are right multiplicatively neutral in* K*.*

(ii) $D \cup \{0_K\}$ *is a right ideal of* K*.*

(iii) E *is an ideal of* K*.*

(iv) K *is additively idempotent.*

(v) *The relation* $(D \times D) \cup (E \times E)$ *is the greatest proper congruence of the (left* K*-) semimodule* ${}_KK$*.*

(vi) *For every* $a \in K$, $aE = \{0_K\}$, $aD = \{a\}$ *and* $aK = \{0_K, a\}$.

Proof. (i) It follows from 5.2(v) that $G_e = \}e\}$ for every $e \in I_m(K)^*$. Now, 4.14 implies $D = I_m(K)^*$. The rest follows from 5.2(ii).

(ii) This follows immediately from (i).

(iii) Easy to see.

(iv) If $a \in K$ and $b \in D$ then $a + a = ab + ab = a(b + b) = a$ (we have $2b \in D$).

(v) and (vi) These assertions are obvious. □

5.4 Assume that $K(+)$ is not a group, $KK \neq \{0_K\}$ and $D = I_m(K)^*$ (see 5.3). Then the assertions 5.3(i),...,(vi) are true and we define a relation ϑ on K by $(a, b) \in \vartheta$ iff $\{ c \in S \mid ca \in E \} \subseteq \{ c \in S \mid cb \in E \}$.

Lemma 5.4.1. *ϑ is reflexive and transitive. Moreover, $(a, b) \in \vartheta$, provided that $b \leq a$.*

Proof. If $b \leq a$ and $ca \in E$ then $cb \in E$, since $cb \leq ca$. □

Lemma 5.4.2. *If $(a, b) \in \vartheta$ then $(a+c, b+c) \in \vartheta$ and $(da, db) \in \vartheta$ for all $c \in K$ and $d \in S$.*

Proof. Use 5.3(i),(iii). □

Lemma 5.4.3. $(0_K, a) \notin \vartheta$ *for every* $a \in K^*$. □

Lemma 5.4.4. (i) $\sigma = \ker(\vartheta)$ *is a congruence of the (left S-) semimodule $_SK$.*

(ii) $(0_K, a) \notin \sigma$ *for every* $a \in K^*$.

Proof. Use 5.4.1, 5.4.2, and 5.4.3. □

Lemma 5.4.5. *σ is the (unique) greatest proper congruence of the (left S-) semimodule $_SK$ and $\sigma \subseteq (D \times D) \cup (E \times E)$.*

Proof. Let τ be a congruence of $_SK$ such that $\tau \nsubseteq \sigma$. Take $(a, b) \in \tau \setminus \sigma$ and assume that $ca \notin E$ and $cb \in E$ for some $c \in S$ (the other case being symmetric). Now, $ca \in D$, $dca = d$ and $dcb = 0_K$ for every $d \in K$. Consequently, $(d, 0_K) \in \tau$ and $\tau = K \times K$. □

Corollary 5.4.6. *The (left S-) semimodule $_SK$ is simple iff $\sigma = \mathrm{id}_K$.* □

Corollary 5.4.7. *The factorsemimodule $_SK/\sigma$ is both minimal and simple.* □

Lemma 5.4.8. *Let $a \in K$ and $F_a = \{\, f \in S \mid fa \in E \,\}$. Then:*
(i) $F_a + F_a \subseteq F_a$ *and* $KF_a \subseteq E_a$.
(ii) $S + (S \setminus F_a) \subseteq S \setminus F_a$.
(iii) $E \subseteq F_a$.
(iv) $F_a = S$ *iff* $a = 0_K$.
(v) $K \subseteq F_a$ *iff* $a \in E$.
(vi) *If* $a \in D$ *then* $K \cap F_a = \{0_K\}$.

Proof. It is easy (use 5.3). □

Lemma 5.4.9. *Let $a \in K$ be such that $b = o_F \in F = F_a$. Then, for every $c \in K$, we have:*
(i) $cba_1 = 0_K$ *for every* $a_1 \in K$ *such that* $(a, a + a_1) \in \sigma$.
(ii) $cba_2 = c$ *for every* $a_2 \in K$ *such that* $(a, a + a_2) \notin \sigma$.

Proof. (i) We have $b \in F_a = F_{a_1+a}$, and so $b \in F_{a_1}$, $ba_1 \in E$ and $cba_1 = 0_K$.

(ii) We have $F_{a+a_2} \subset F_a$, and hence $b_1 a \in E$ and $b_1 a_2 \notin E$ for some $b_1 \in S$. Now, $b_1 + b = b$, $ba \in E$, $ba_2 \in D$ and $cba_2 = c$. □

6. Partial summary (b)

Let S be a semiring and K be a minimal ideal of S such that $B = \{o_K\}$ (see 3.4). We put $K^\circ = K \setminus \{o_K\}$ and $I_m(K)^\circ = I_m(K) \setminus \{o_K\}$.

Proposition 6.1. (i) $o_K K = \{o_K\} = S o_K$.
(ii) $o_K S \subseteq \underline{R}(S$.
(iii) $Sa = K$ *for every* $a \in K^\circ$.
(iv) $o_K \in L_1 = \{\, a \in S \mid aK = \{o_K\} \,\}$ *and L is an ideal of S.*
(v) *If $K \subseteq L_1$ then $KK = \{o_K\}$ and $K \times K \subseteq \varrho$, where ϱ is the congruence of S defined by $(a, b) \in \varrho$ iff $ac = bc$ for every $c \in K$.*
(vi) *If $K \subseteq L_1$ and $\varrho = S \times S$ then $SK = \{o_K\}$.*
(vii) *If $SK = \{o_K\}$ (or $L_1 = S$) then either $|K| = 2$ or $K(+)$ is a finite (cyclic) group of prime order.*
(viii) *If $K \nsubseteq L_1$ then $L_1 K = L_1 \cap K = \{o\}$.*
(ix) *If $|\underline{R}(S)| = 1$ then o_K is multiplicatively absorbing in S, $S + o_K$ is a bi-ideal of S and $K \nsubseteq S + o_K$.*
(x) *If $S = o_K = \{o_K\}$ then $o_K = o_S$.*
(xi) $E = \{\, a \in K \mid |Ka| = 1 \,\} = \{\, a \in K \mid Ka = \{o_K\} \,\}$.
(xii) $E = K$ *iff* $\subseteq L_1$ (see (v) and (vi)).
(xiii) $DD = D = \{\, a \in K \mid Ka = K \,\}$ *and $Da = D$ for every $a \in D$.*
(xiv) $K = E \cup D$ *and* $E \cap D = \emptyset$.

(xv) $o_K \notin K^\circ D$.

(xvi) *Either* K *is multiplicatively idempotent or* $2a \neq a$ *for every* $a \in K^\circ$.

(xvii) *Either* $2a = o_K$ *for every* $a \in K$, *or* $2b \neq o_K$ *for every* $b \in K^\circ$ *and* $K = \{\, 2a \mid a \in K \,\}$.

(xviii) *If* $a \in I_m(K)^\circ$ *then* a *is right multiplicatively neutral in* K.

(xix) $I_m(K)^\circ \subseteq D$.

Proof. See 3.4, 3.6, 3.9 and 4.2, 4.3, 4.4. □

Proposition 6.2. (i) *For every* $e \in I_m(K)^\circ$, *the set* $H_e = \{\, a \in K^\circ \mid ea = a \,\}$ *is a subgroup of the multiplicative semigroup* $K(\cdot)$ *and* e *is the multiplicatively neutral element of* H_e. *Moreover,* $H_e \subseteq D$.

(ii) $H_e^+ = eK = H_e \cup \{o_K\}$ *is a right ideal of* K.

(iii) *If* $a \in H_e$ *is such that* $a^m = a^n$ *for some* $1 \leq m < n$ *then either* $a = e$ *or* $o_K = a + a^2 + \cdots + a^{(n-m)m}$.

(iv) *If* $e, f \in I_m(K)^\circ$, $e \neq f$, *then* $H_e \cap H_f = \emptyset$ *and the mapping* $H_e \to fH_e = H_f$ *is an isomorphism of the multiplicative groups.*

(v) *If* $e, f \in I_m(K)^\circ$ *then the mapping* $H_e^+ \to fH_e^+ = H_f^+$ *is an isomorphism of the semirings.*

Proof. See 4.9. 4.11, 4.12, 4.13 and 4.15. □

Lemma 6.3. *Let* $e \in I_m(K)^\circ$ *be such that* $2e = o_K$. *Then* $2K = \{o_K\} = H_e + H_e$.

Proof. First, $2K = \{o_K\}$ by 6.1(xvii). Next, $(a+e)^2 = a^2 + 2a + e = o_K$ for $a \in H_e$, and hence $a + e = o_K$ and $ab + b = o_K$ for all $a, b \in H_e$. Thus $H_e + H_e = \{o_K\}$ □

Lemma 6.4. *Let* $e \in I_M(K)^\circ$ *be such that* $e \in F_e = \{\, a \in H_e \mid a + e \neq o_K \,\}$. *Then:*

(i) F_e *is a subsemiring of* K *and the multiplicative semigroup of* F_e *is a group.*

(ii) *If* $F_e \neq \{e\}$ *then the multiplicative group of* F_e *is infinite and torsionfree.*

(iii) *If* $F_e = \{e\}$ *then* $2a = a$ *and* $a + b = o_K$ *for all* $a, b \in H_e$, $a \neq b$.

Proof. (i) We have $a + e \in H_e$ for every $a \in H_e$. Now, $e + a + b + ab = (a+e)(b+e) \in H_l$ for $a, b \in H_e$, and hence $a + b \in F_e$ and $ab \in F_e$. If $c \in H_e$ is such that $ac = e$ then $o_K \neq (a+e)c = e + c$, so that $c \in F_e$.

(ii) Use 6.2(iii).

(iii) If $c \in H_e$ is such that $ac = e$ then $(a+b)c = e + bc$ and $bc \neq e$. Since $F_e = \{e\}$, we have $e + bc = o_K$, and hence $a + b = o_K$ as well. Of course, $2e = e$ by (i). □

Proposition 6.5. *Assume that* $KK \neq \{o_K\}$ *and no multiplicative subsemigroup of* D *is a copy of the additive semigroup of positive integers. Then:*

(i) $D \neq \emptyset$ *and* $Da = D$ *for every* $a \in D$.

(ii) $D = \bigcup H_e$, $e \in I_m(K)^\circ$.

(iii) *For every* $e \in I_m(K)^\circ$, *the multiplicative group of* H_e *is periodic.*

(iv) $a + b = o_K$ *for all* $a, b \in H_e$, $a \neq b$.

(v) *If* $2e \neq o_K$ *then* $2a = a$ *for every* $a \in H_e$.

(vi) *If* $2e = o_K$ *then* $a + b = o_K$ *for all* $a, b \in H_e$.

Proof. (i) See 6.1(xii),(xiii).

(ii) This is 4.14.

(iii) This follows immediately from our assumption.

(iv), (v) and (vi). If $2e = o_K$ then 6.3 applies. If $2e \neq o_K$ then $F_e = \{e\}$ by 6.4(ii) and 6.4(iii) applies. □

Proposition 6.6. *Assume that* K *is multiplicatively idempotent and* $\emptyset \neq D = I_m(K)^\circ$. *Then:*

(i) D *is a subsemiring of* K.

(ii) *If* $a, b \in K$ *are such that* $a \leq b$ *and* $b \in D$ *then* $a \in D$.

(iii) E *is a bi-ideal of* K.

(iv) $aD = \{a\}$ *and* $aE = \{o_K\}$ *for every* $a \in K$.

Proof. Easy (use 4.5). □

6.7 Assume that $KK \neq \{o_K\}$ and no multiplicative subsemigroup of D is a copy of the additive semigroup of positive integers (see 6.5).

Lemma 6.7.1. (i) $DD = D$.

(ii) $KE = \{o_K\}$.

(iii) $Da = D$ *and* $Ea = E$ *for every* $a \in D$.

(iv) *If* $a, b \in K$ *are such that* $ab \in E$ *then either* $a \in E$, *or* $b \in E$ *and* $ab = o_K$.

Proof. (i) See 6.1(xiii).

(ii) See 6.1(xi).

(iii) We have $K = Ka = Da \cup Ea$, where $Da \subseteq D$ and $Ea \subseteq E$. Thus $Da = D$ and $Ea = E$.

(iv) This follows immediately from (i). □

Lemma 6.7.2. *Let* $a \in D$. *Then:*

(i) $a \in H_e$ *for a uniquely determined* $e \in IU_m(K)^\circ$.

(ii) $H_f a = H_f$ *for every* $f \in I_m(K)^\circ$.

(iii) $aH_f = H_f$.

(iv) $aD = H_e$ *and* $aK = H_e^+ = H_e \cup \{o_K\}$.

Proof. (i) By 6.5(ii), $a \in G_e$ and, by 6.2(iv), the idempotent e is determined uniquely.

(ii) We have $H_f a \subseteq DD \subseteq D$ by 6.7.1(i) and $fba = ba$ for every $b \in H_f$. Thus $H_f a \subseteq H_f$. Since $Da = D$, we get $H_f a = H_f$.

(iii) Clearly, $aH_f \subseteq H_e$. On the other hand, if $b \in H_e$ then $b = ac$ for some $c \in H_e$ (see 6.2(i)), and hence $b = afc$, while $fc \in H_f$ (use 6.1(xviii).

(iv) This follows from (iii). □

References

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

Accepted: 13.11.2019