CONGRUENCE-SIMPLE SEMIRINGS

ROBERT EL BASHIR AND TOMÁŠ KEPKA

Abstract. Several classes of congruence-simple semirings are characterized and various further examples are constructed. Among others, it is shown that every congruence-simple semiring fits into one of the following three classes: additively idempotent semirings, additively cancellative semirings, additively nil-semirings of index 2.

Keywords: semiring, congruence relation.

Congruence-simple semirings were scarcely studied so far ([6], [7], [9], [18], [20], [21]), although at least one of them is commonly known and used in everyday practice. Henceforth, the purpose of this note is to initiate the study of (generally non-commutative) congruence-simple semirings. As concernes background of the theory of semirings, a reader is referred to [9], [12] and [13].

1. Preliminaries

A semiring is a non-empty set equipped with two associative operations (usually denoted as addition and multiplication) such that the addition is commutative and the multiplication distributes over the addition.

Let S be a semiring. A relation $r \subseteq S \times S$ is a congruence of S if r is an equivalence and $(a+c, b+c) \in r$, $(ac, bc) \in r$, $(ca, cb) \in r$ for all $(a, b) \in r$ and $c \in S$. A non-empty subset I of S is an ideal (bi-ideal) of S if $(I+I) \cup SI \cup IS \subseteq I$ $((S+I) \cup SI \cup IS \subseteq I)$. The semiring S will be called congruence-simple if S has just two congruence relations. The semiring S will be called ideal-simple (bi-ideal-simple) if $|S| \geq 2$ and $I = S$, whenever I is an ideal (bi-ideal) of S such that $|I| \geq 2$.

Lemma 1.1. *Every congruence-simple and/or ideal-simple semiring is bi-ideal-simple.*

Proof. If I is a bi-ideal of S, then the relation $(I \times I) \cup \mathrm{id}_S$ is a congruence of S. □

Proposition 1.2. *Let R be a ring (i.e., R is a semiring and $R(+)$ is a group). Then the following conditions are equivalent:*

(i) *R is congruence-simple as a ring.*
(ii) *R is congruence-simple as a semiring.*
(iii) *R is ideal-simple as a ring.*
(iv) *R is ideal-simple as a semiring.*

This work is a part of the research project MSM 0021620839 financed by MŠMT and partly supported by the Grant Agency of Czech Republic, Grant No. 201/05/0002.

Proof. We show only that (iii) implies (iv), the other implications being immediately clear. Now, let R be ideal-simple as a ring and let I be an ideal of R as a semiring. The set $K = \{a \in I\ ;\ -a \in I\}$ is non-empty and it is an ideal of R as a ring. If $K = R$, then $I = R$, and hence we assume that $K = 0$. However, $RI \cup IR \subseteq K$ and consequently $I \subseteq L = \{a \in R\ ;\ Ra \cup aR = 0\}$. If $L = 0$, then $I = 0$. If $L \neq 0$, then $L = R$ (since L is an ideal of the ring R) and R is a zero multiplication ring. But then R is of finite prime order and every semiring ideal of R is a ring ideal. $\square$

Note also that every two-element semiring is both congruence- and ideal-simple and that there exist just ten two-element semirings Z_1, ..., Z_{10} up to isomorphism (the first eight of them being commutative).

Z_1 :

+	0	1
0	0	0
1	0	0

.	0	1
0	0	0
1	0	0

Z_2 :

+	0	1
0	0	0
1	0	0

.	0	1
0	0	0
1	0	1

Z_3 :

+	0	1
0	0	0
1	0	1

.	0	1
0	0	0
1	0	0

Z_4 :

+	0	1
0	0	0
1	0	1

.	0	1
0	1	1
1	1	1

Z_5 :

+	0	1
0	0	0
1	0	1

.	0	1
0	0	1
1	1	1

Z_6 :

+	0	1
0	0	0
1	0	1

.	0	1
0	0	0
1	0	1

Z_7 :

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	0

Z_8 :

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

Z_9 :

+	0	1
0	0	0
1	0	1

.	0	1
0	0	1
1	0	1

Z_{10} :

+	0	1
0	0	0
1	0	1

.	0	1
0	0	0
1	1	1

An element w of a semiring S is called additively (multiplicatively) neutral if $w + a = a$ ($wa = a = aw$) for every $a \in S$. Such an element, if it exists, is unique and is usually denoted by the symbol 0 ($= 0_S$) (1 ($= 1_S$)) and is occassionally named a zero (unit) element of the semiring S.

An element $w \in S$ is called additively (multiplicatively) absorbing if $w + a = w$ ($aw = w = wa$) for every $a \in S$. The element w is called bi-absorbing if it is both additively and multiplicatively absorbing. Clearly, there exists at most one bi-absorbing element in S and it will be denoted by the symbol o ($= o_S$) in the sequel.

An element $w \in S$ is bi-absorbing if and only if $\{w\}$ is a bi-ideal of S.

If $w \in S$ is multiplicatively absorbing, then $2w = w+w = w^2+w^2 = w(w+w) = w$ and $\{w\}$ is an ideal of S. Consequently, w is multiplicatively absorbing if and only if $\{w\}$ is an ideal of S.

If $w \in S$ is additively absorbing, then $w^4 = w^2$, but it may happen that $w \neq w^2$ (e.g., in Z_4), and so $\{w\}$ neednot be a subsemiring of S.

Proposition 1.3. *Let S be a non-trivial semiring such that either S is finitely generated or S is bi-ideal-simple and $o_S \in S$. Then there exists at least one congruence r of S such that S/r is a congruence-simple semiring.*

Proof. We have to show that S has at least one maximal congruence. The proof is divided into five parts.

(i) Assume that the semiring S is generated by a one-element set $\{a\}$ such that $a+a = a \neq aa = b$ ($b = a+a \neq a = aa$) and consider a congruence r of S maximal with respect to $(a,b) \notin r$. Then $r \neq S \times S$ and, if s is a congruence of S such that $r \subseteq s \neq r$, then $(a,b) \in s$ and it follows easily that S/s is a one-element semiring, i.e., $s = S \times S$. Thus r is a maximal congruence of S.

(ii) Assume that S is generated by a one-element set $\{a\}$ such that $b = a+a \neq a$ and consider a congruence t of S maximal with respect to $(a,b) \notin t$. If t is not a maximal congruence of S, then there exists a congruence s of S such that $t \subseteq s \neq t$ and $s \neq S \times S$. Now, $(a,b) \in s$ due to the choice of t and $(a, aa) \notin s$ due to the inequality $s \neq S \times S$. Consequently, it follows from (i) that $s \subseteq r$ for at least one maximal congruence r of S.

(iii) Assume that S is generated by a one-element set $\{a\}$. Since S is non-trivial, we have either $a + a \neq a$ or $a + a = a \neq aa$. Thus either (ii) or (i) applies.

(iv) Assume that S is generated by a non-empty finite set M. If $|M| = 1$, then (iii) applies. On the other hand, if $\{a,b\} \subseteq M$, $a \neq b$, and if t is maximal with respect to $(a,b) \notin t$, then either t is a maximal congruence of S or there exists a congruence s of S such that $t \subseteq s \neq t$ and $s \neq S \times S$. In that case, the factor-semiring S/s is non-trivial and can be generated by at most $|M| - 1$ elements.

(v) Assume that S is bi-ideal-simple and $o \in S$. Take $a \in S$, $a \neq o$, and consider a congruence r of S maximal with respect to $(a,o) \notin r$. Then $r \neq S \times S$ and, if s is a congruence of S such that $r \subseteq s \neq r$, then $(a,o) \in s$, $\{a,o\} \subseteq I = \{v \in S\ ;\ (v,o) \in s\}$ and $|I| \geq 2$. On the other hand, it is easy to see that I is a bi-ideal of S, and hence $I = S$, since S is bi-ideal-simple. Consequently, $s = S \times S$ and it follows that r is a maximal congruence of S. □

A semiring S is called additively
- idempotent if $a + a = a$ for every $a \in S$;
- cancellative if $a + b \neq a + c$ for all $a, b, c \in S$, $b \neq c$;
- zeropotent if $2a + b = 2a$ for all $a, b \in S$;
- constant if $a + b = a + c$ for all $a, b, c \in S$.

Lemma 1.4. *Let S be an additively constant (zeropotent) semiring. Then S contains a bi-absorbing element o and $a + b = o$ ($a + a = o$) for all $a, b \in S$.*

Proof. Easy. □

Lemma 1.5. *Let S be a bi-ideal-simple semiring containing a multiplicatively absorbing element w. Then just one of the following two cases takes place:*

(1) w is a bi-absorbing element of S and $S + SvS = S$ for every $v \in S$, $v \neq w$;

(2) w is an additively neutral element of S and $S + SvS = S$ for every $v \in S$.

Proof. Firstly, $w = w(w + w) = w^2 + w^2 = w + w$. Next, assume that w is not additively absorbing. Then $S+w \neq \{w\}$, and therefore $|S+w| \geq 2$, since $w \in S+w$. But $S + w = S + SwS$ is a bi-ideal of S, and hence $S + w = S$. Since $w = w + w$, we conclude that w is additively neutral. The rest is clear. □

Lemma 1.6. *Let A be a non-trivial semigroup containing an element w such that the subset $A \setminus \{w\}$ is a subgroup of A. Then at least one of the following conditions holds:*

(1) A is a two-element semigroup;

(2) w is an absorbing element of A;

(3) w is a neutral element of A;

(4) There exists $v \in A$ such that $v \neq w$ and $wx = vx$, $xw = xv$ for every $x \in A$ (then $w^2 = v^2$ and the relation $\{(w, v), (v, w)\} \cup \mathrm{id}_A$ is a congruence of A).

Proof. Easy. □

Lemma 1.7. *Let S be a non-trivial semiring containing an element w such that the set $T = S \setminus \{w\}$ is a subgroup of the multiplicative semigroup of S (cf. 1.6).*

(i) If w is multiplicatively but not additively absorbing, then w is additively neutral and either S is a division ring or T is a subsemiring of S and $(T \times T) \cup \mathrm{id}_S$ is a congruence of S.

(ii) If w is multiplicatively neutral, then T is a subsemiring of S and $\{(w, e), (e, w)\} \cup \mathrm{id}_S$ is a congruence of S, where e denotes the unit element of the group $T(\cdot)$.

Proof. (i) Clearly, S is bi-ideal-simple, and hence w is additively neutral by 1.5. If $T+T \subseteq T$, then $(T\times T)\cup\mathrm{id}_S$ is a congruence of S. On the other hand, if $a+b = w$ for some $a, b \in T$, then $ac + bc = w$ for every $c \in T$ and it follows easily that $S(+)$ is a group. Thus S is a ring.

(ii) If $a+b = w$ for some $a, b \in T$, then $e = we = (a+b)e = ae+be = a+b = w$, a contradiction. Thus $T + T \subseteq T$ and T is a subsemiring of S. Further, $a + e = ae+we = (a+w)e$ for every $a \in T$. If $a+w = w$, then $a+e = e$. If $a+w \neq w$, then $a + e = a + w$. Now, we conclude easily that $\{(w, e), (e, w)\} \cup \mathrm{id}_S$ is a congruence of S. □

1.8. Let I be an ideal of a semiring S. Define two relations r and s on S in the following way:

(1) $(u, v) \in r$ iff $\{u\} \cup (u + I) = \{v\} \cup (v + I)$;

(2) $(u, v) \in s$ iff $u + I = v + I$.

Lemma 1.8.1. *(i) r is a congruence of the semiring S and $(u, v) \in r$ iff either $u = v$ or $u = v + a$ and $v = u + b$ for some $a, b \in I$.*

(ii) s is an equivalence and s is compatible with the addition.

(iii) $r \subseteq s$.

Proof. (i) Clearly, r is an equivalence and $r \subseteq t$, where t is defined by $(u, v) \in t$ iff either $u = v$ or $u \in v + I$ and $v \in u + I$. Conversely, if $u = v + a$ and $v = u + b$, $a, b \in I$, then $u + I = v + a + I \subseteq v + I = u + b + I \subseteq u + I$, and therefore $u + I = v + I$, $\{u\} \cup (u + I) = \{v\} \cup (v + I)$ and $(u, v) \in r$. Thus $r = t$. Finally, it is easy to check that the relation t is compatible with respect to the addition and multiplication.

(ii) Obvious.

(iii) The inclusion was already proved in (i). □

Lemma 1.8.2. *(i) If $I(+)$ is a subgroup of $S(+)$, then s is a congruence of the semiring S.*

(ii) If S has an additively neutral element and $0_S \in I$, then $r = s$ (and hence s is a congruence of S).

Proof. Easy to see. □

Lemma 1.8.3. *(i) If $(u, v) \in r$, $u \neq v$, then there is $c \in S$ with $u = u + c$ and $v = v + c$.*

(ii) If S is additively cancellative and $r \neq \mathrm{id}_S$, then S has an additively neutral element, $0_S \in I$ and $r = s$.

(iii) If $I(+)$ is a subgroup of $S(+)$, then I is contained in a block of r and s is a congruence of S.

(iv) If S is additively cancellative and $I(+)$ is a subgroup of S, then $0_S \in I$ and I is a block of $r = s$.

Proof. Easy (use 1.8.2). □

Lemma 1.8.4. *Assume that $s = S \times S$. Then there exists a bi-ideal K of S such that the following conditions are satisfied:*

(i) $K \subseteq I$.
(ii) $x + I = K = x + K$ for every $x \in S$.
(iii) $K(+)$ is a subgroup of $S(+)$.
(iv) K is a subring of S.

Proof. Since $s = S \times S$, there is a subset K of S such that $x + I = K$ for every $x \in S$. Now, $x+K = 2x+I = K$, $xK = x^2+xI \subseteq x^2+I = K$ and $Kx = x^2+Ix \subseteq x^2+I = K$ and we see that K is a bi-ideal of S. Moreover, $a+K = K = a+I \subseteq I$ for every $a \in K$ and it follows that $K(+)$ is a subgroup of $S(+)$ and K a subring of S. □

Lemma 1.8.5. *Assume that S is bi-ideal-simple and $s = S \times S$. Then either $K = \{o_S\}$ and $S + I = \{o_S\}$ or S is a ring and $K = I = S$.*

Proof. Use 1.8.4. □

Lemma 1.8.6. *If $r = S \times S$, then S is a ring and $I = S$.*

Proof. We have $s = S \times S$ and we put $0 = 0_K$ (see 1.8.4 (iii)). If $u, v \in S$, $u \neq v$, then $u \in v + I = v + K$, $v \in u + I = u + K$ and $u = v + a$, $v = u + b$ for some $a, b \in K$. Now, $u = u + c$ and $v = v + c$, where $c = a + b$, and we get $u + 0 = u + c + 0 = u + c = u$. Thus $0 = 0_S$ and $u = u + 0 \in u + K = K$. Consequently, $K = S$. □

2. Basic classification

Theorem 2.1. *Let S be a congruence-simple semiring. Then just one of the following five cases takes place:*

(1) *S is additively idempotent;*
(2) *S is additively cancellative;*
(3) *S is additively zeropotent and $S + S = S$;*
(4) *S is additively constant and $SS = S$;*

(5) *S is isomorphic to the two-element semiring Z_1.*

Proof. First, define a relation r on S by $(x,y) \in r$ if and only if $2x = 2y$. Then r is a congruence of S and we have either $r = \mathrm{id}_S$ or $r = S \times S$.

Assume $r = \mathrm{id}_S$ and define a relation s by $(x,y) \in s$ if and only if $2^i x = y + u$ and $2^j y = x + v$ for some $i, j \geq 0$ and $u, v \in S \cup \{0\}$. Again, s is a congruence of S and S is additively idempotent, provided that $s = \mathrm{id}_S$. On the other hand, if $s = S \times S$, then S is additively cancellative.

Assume $r = S \times S$, put $o = 2x$, $x \in S$, and define a congruence t of S by $(x,y) \in t$ if and only if $3x = 3y$. If $t = \mathrm{id}_S$, then S is additively cancellative, and so assume $t = S \times S$. Then o is a bi-absorbing element of S and the semiring S is additively zeropotent. If $T = S + S \neq S$, then $T = o$ (since T is a bi-ideal of S), SS is a bi-ideal of S and the rest is clear. □

Lemma 2.2. *Let S be a congruence-simple semiring. Then just one of the following three cases holds:*

(1) For all $a, b \in S$, $a \neq b$, there exists $c, d \in S$ with $ac \neq bc$ and $da \neq db$;

(2) S is a zero multiplication ring of finite prime order;

(3) S is isomorphic to one of the two-element semirings Z_1, Z_3, Z_4, Z_9 and Z_{10}.

Proof. Define a relation r on S by $(a,b) \in r$ iff $az = bz$ for every $z \in S$. Then r is a congruence of S and $ac \neq bc$ for at least one $c \in S$, provided that $r = \mathrm{id}_S$. Hence, assume $r \neq \mathrm{id}_S$. Then $r = S \times S$ and there is a transformation f of S such that $xy = f(y)$ for all $x, y \in S$. Clearly, $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ and $f^2(x) = f(x)$. Consequently, f is an endomorphism of S and $s = \ker(f)$ is a congruence of S.

If $s = \mathrm{id}_S$, then $f^2 = f$ implies $f = \mathrm{id}_S$ and $xy = y$ for all $x, y \in S$. Then, of course, $S \simeq Z_9$.

If $s = S \times S$, then f is constant and there is $w \in S$ such that $xy = w$ for all $x, y \in S$. The rest is clear. □

Lemma 2.3. *Let S be a semiring such that S is finitely generated as a bi-ideal. If S contains at least one proper bi-ideal (i.e., S is not as a bi-ideal generated by any element), then there exists a congruence r of S such that S/r is congruence-simple (i.e., r is a maximal congruence of S).*

Proof. S has a proper bi-ideal L and, evidently, $M \nsubseteq L$, where M is a finite set generating S as a bi-ideal. Let K be a bi-ideal maximal with respect to $L \subseteq K$ and $M \nsubseteq K$. The relation $s = (K \times K) \cup \mathrm{id}_S$ is a congruence of S and S/s is a bi-ideal simple semiring with a bi-absorbing element. The result now follows from 1.3. □

Proposition 2.4. *Let I be an ideal of a congruence-simple semiring S. Then just one of the following two cases holds:*

(i) S is a (simple) ring and $I = S$.

(ii) If $u, v \in S$, $u \neq v$, then either $u \notin v + I$ or $v \notin u + I$.

Proof. Let r be the congruence of S corresponding to I as in 1.8. If $r = \mathrm{id}_S$, then (ii) is true by 1.8.1 (i). On the other hand, if $r \neq \mathrm{id}_S$, then $r = S \times S$ and (i) is true by 1.8.6. □

3. Matrix semirings

If S is a semiring and n a positive integer, then $\mathrm{M}_n(S)$ will denote the semiring of square $n \times n$-matrices with entries from S.

Lemma 3.1. *Let S be a semiring such that the matrix semiring $\mathrm{M}_n(S)$ is congruence-simple for some $n \geq 1$. Then S is congruence-simple.*

Proof. Let r be a congruence of S. Define a relation ρ on $\mathrm{M}_n(S)$ by $(A, B) \in \rho$ if and only if $(a_{i,j}, b_{i,j}) \in r$ for all indices i, j, $1 \leq i, j \leq n$. It is easy to check that ρ becomes a congruence of $T = \mathrm{M}_n(S)$. If $\rho = \mathrm{id}_T$, then $r = \mathrm{id}_S$. If $\rho = T \times T$, then $r = S \times S$. Thus S is congruence-simple. □

Lemma 3.2. *Let S be a semiring containing a bi-absorbing element. Then, for every $n \geq 2$, the matrix semiring $\mathrm{M}_n(S)$ is not bi-ideal-simple (and consequently it is not congruence-simple either).*

Proof. We may assume that S is non-trivial. Then $I = \{A \in \mathrm{M}_n(S)\ ;\ a_{i,j} = o_S,\ (i,j) \neq (1,1)\}$ is a proper non-trivial bi-ideal of $\mathrm{M}_n(S)$. □

Lemma 3.3. *Let S be a multiplicatively constant semiring (i.e., $|SS| = 1$). Then, for every $n \geq 2$, the matrix semiring $\mathrm{M}_n(S)$ is not congruence-simple.*

Proof. Assume, on the contrary, that $T = \mathrm{M}_n(S)$ is congruence-simple. Clearly, T is multiplicatively constant, too, and it follows from 2.2 that T is finite of prime order. On the other hand, $|T| = m^{n^2}$, $m = |S|$, a contradiction. □

Proposition 3.4. *Let a semiring S and an integer $n \geq 2$ be such that the matrix semiring $\mathrm{M}_n(S)$ is congruence-simple. Then:*
(i) S is congruence-simple.
(ii) S contains no bi-absorbing element.
(iii) S is not multiplicatively constant.
(iv) S is either additively idempotent or additively cancellative.

Proof. Combine 3.1, 3.2, 3.3 and 2.1. □

4. Congruence-simple additively idempotent semirings

Construction 4.1. Let S $(= S(\cdot))$ be a multiplicative semigroup containing an absorbing element o. Define an addition on S by $x + y = o$ and $x + x = x$ for all $x, y \in S$, $x \neq y$. In this way we obtain an additively idempotent associative algebraic structure $\mathrm{V}(S(\cdot)) = S(+, \cdot)$ and o becomes a bi-absorbing element.

Lemma 4.1.1. $\mathrm{V}(S(\cdot))$ *is a semiring if and only if the semigroup $S(\cdot)$ satisfies:*

(V) *If $a, b, c \in S$ are such that $b \neq c$ and $ab = ac$ ($ba = ca$), then $ab = o$ ($ba = o$).*

Proof. Easy. □

Lemma 4.1.2. *A non-empty subset I of S is a bi-ideal of* $\mathrm{V}(S(\cdot))$ *if and only if it is an ideal of $S(\cdot)$.*

Proof. Obvious. □

Proposition 4.1.3. *Assume that* (V) *is true and put* $S = S(+,\cdot) = \mathrm{V}(S(\cdot))$. *The following conditions are equivalent:*

(i) The semiring S *is congruence-simple.*

(ii) The semiring S *is bi-ideal-simple.*

(iii) The semigroup $S(\cdot)$ *is ideal-simple.*

Proof. (i) implies (ii) by 1.1 and (ii) is equivalent to (iii) by 4.1.2. Now, assume that S is bi-ideal-simple and consider a non-identical congruence r of the semiring. There are $a, b \in S$ such that $a \neq b$, $(a, b) \in r$ and we put $I = \{v \in S \ ; \ (v, o) \in r\}$. If $o \in \{a, b\}$, then $|I| \geq 2$. If $o \notin \{a, b\}$, then $a + a = a \neq o = a + b$, $(a, o) \in r$ and $|I| \geq 2$ again. Thus $|I| \geq 2$ and $I = S$, since I is a bi-ideal. Consequently, $r = S \times S$. □

Example 4.1.4. Let T be an ideal-simple cancellative semigroup (e.g., a group), $o \notin T$, $S = T \cup \{o\}$, while o is an absorbing element of S. Then S is an ideal-simple semigroup satisfying the condition (V).

Proposition 4.2. *Let* S *be a congruence-simple additively idempotent semiring containing an element* o *such that* $x + y = o$ *for all* $x, y \in S$, $x \neq y$. *Then either* S *is isomorphic to one of the two-element semirings* Z_4, Z_5, Z_9 *and* Z_{10} *or the element* o *is bi-absorbing,* $S(\cdot)$ *is an ideal-simple semigroup satisfying* (V) *and* $S = \mathrm{V}(S(\cdot))$ *(see 4.1).*

Proof. We may assume that $|S| \geq 3$. The rest of the proof is divided into four parts.

(i) Put $A_l = \{x \in S \ ; \ xo \neq o\}$, $A_r = \{x \in S \ ; \ ox \neq o\}$, $B_l = \{x \in S \ ; \ xy = x^2 \text{ for every } y \in S\}$ and $B_r = \{x \in S \ ; \ yx = x^2 \text{ for every } y \in S\}$. Then $A_l \subseteq B_l$ and $A_r \subseteq B_r$.

(ii) Assume that $A_l \neq \emptyset \neq A_r$. Then there is an element $w \in S$ such that $x^2 = w$ for every $x \in B_l \cup B_r$, $So \cup oS \cup SoS \subseteq \{w, o\} = P$ and P is a bi-ideal of S. Since $|S| \geq 3$ and S is congruence-simple, it follows that $|P| = 1$, $w = o$ and $A_l = \emptyset$, a contradiction.

(iii) Assume that $A_l \neq \emptyset = A_r$. Then $ox = o$ for every $x \in S$, $o \in B_l$, $|B_l| \geq 2$, B_l is a bi-ideal of S and consequently $B_l = S$. That is, there is a transformation t of S such that $xy = t(x)$ for all $x, y \in S$. Since $S(\cdot)$ is associative, we have $t^2 = t$. Clearly, $t(S)$ is a bi-ideal of S and, if $t(S) = o$, then $|S| = 2$, a contradiction. On the other hand, if $t(S) = S$, then $t = \mathrm{id}_S$ and $|S| = 2$ again.

(iv) We have proven that $A_l = \emptyset = A_r$, i.e., $xo = o = ox$ for every $x \in S$. Now, it follows easily that $S(\cdot)$ is an ideal-simple semigroup satisfying (V). □

Proposition 4.3. ([7, 3.3]) *Let* S *be a congruence-simple commutative additively idempotent semiring containing an additively absorbing element* o. *Then either* S *is isomorphic to one of the two-element semirings* Z_3, Z_4 *and* Z_5 *or* o *is a bi-absorbing element,* $T = S \setminus \{o\}$ *is an (abelian) subgroup of the multiplicative semigroup* $S(\cdot)$, $x + y = o$ *for all* $x, y \in S$, $x \neq y$, *and* $S = \mathrm{V}(S(\cdot))$ *(see 4.1).*

Construction 4.4. Let $T = T(\cdot, \leq)$ be an ordered group satisfying the following condition:

(Z) If $a, b, c \in T$ are such that $c \leq a$ and $c \leq b$, then $\inf(a, b) = a \wedge b$ exists in $T(\leq)$.

Further, let $o \notin T$, $S = T \cup \{o\}$ and $o \leq a$ for every $a \in T$. Then $x + y = x \wedge y$ exists for all $x, y \in S$ and the algebra $S = S(+, \cdot)$ is a bi-ideal-simple additively idempotent semiring, while the element o is bi-absorbing. The unit element $1 = 1_T$ of $T(\cdot)$ becomes a multiplicatively neutral element of the semiring.

For $x \in S$, put $A(x) = \{y \in S \ ; \ x + y = o\}$.

Lemma 4.4.1. *(i) $A(o) = S$.*
(ii) $a \notin A(a)$ and $A(a) \neq S$ for every $a \in T$.
(iii) If $a, b \in T$, then $a \in A(b)$ iff $b \in A(a)$ and iff $a \wedge b$ does not exist in $T(\leq)$.
(iv) $A(a) = aA(1) = A(1)a$ for every $a \in T$.
(v) The set $A(1) \setminus \{o\}$ is a normal subset of the group T.
(vi) The set $\{a \ ; \ a \in T, A(a) = A(1)\}$ is a normal subgroup of the group T.

Proof. Easy. □

Define a relation ρ on S by $(x, y) \in \rho$ iff $A(x) = A(y)$.

Lemma 4.4.2. *The relation ρ is a congruence of the semiring S, $\rho \neq S \times S$ and the factor-semiring S/ρ is congruence-simple (i.e., ρ is a maximal congruence of S).*

Proof. It follows easily from 4.4.1 that ρ is a congruence of S and $\rho \neq S \times S$, i.e., S/ρ is a non-trivial semiring. Let r be a congruence of S such that $\rho \subseteq r \neq \rho$. The set $I = \{x \ ; \ (x, o) \in r\}$ is a bi-ideal of S, and hence $I = S$ and $r = S \times S$, provided that $I \neq \{o\}$. Now, assume $I = \{o\}$ and take $(u, v) \in r \setminus \rho$. Then $u, v \in T$ and there is $a \in T$ such that $u + a \neq v + a$ and either $u + a = o$ or $v + a = o$. Thus $\{u + a, v + a\}$ is a two-element subset of I, a contradiction. □

Corollary 4.4.3. *The following conditions are equivalent:*
(i) The semiring S is congruence-simple.
(ii) $\rho = \mathrm{id}_S$.
(iii) $A(1) \neq aA(1)$ (or $A(1) \neq A(1)a$) for every $a \in T$, $a \neq 1$,

Construction 4.5. Let $S = S(\cdot, \leq)$ be an ordered non-trivial group such that the ordered set $S(\leq)$ is a lower semilattice. Setting $a + b = a \wedge b$ $(= \inf(a, b))$ for all $a, b \in S$, we get a bi-ideal-simple additively idempotent semiring $S = S(+, \cdot)$ with a multiplicatively neutral element.

Lemma 4.5.1. *The semiring S is infinite and has no additively and no multiplicatively absorbing element. The semiring has no additively neutral element either.*

Proof. Easy. □

Remark 4.5.2. The semiring S is congruence-simple, provided that the group $S(\cdot)$ is simple. Examples of linearly ordered simple groups can be found in [3], [5], [14] and elsewhere.

Construction 4.6. Let $S = S(\cdot, \leq)$ be a linearly ordered semigroup. Setting $a + b = \min(a, b)$ we get an additively idempotent semiring $\mathrm{W}(S(\cdot, \leq)) = S(+, \cdot)$. This semiring is additively quasitrivial, i.e., $a + b \in \{a, b\}$ for all $a, b \in S$, and hence it is additively semisubtractive.

Example 4.6.1. Let $S(+,\leq)$ be a subsemigroup of the additive group $\mathbb{R}(+)$ of real numbers together with the usual order. According to [7, 5.1.1], the semiring $\mathrm{W}(S(+,\leq))$ is congruence-simple if and only if $S\cap\mathbb{R}^+\neq\emptyset\neq S\cap\mathbb{R}^-$ (notice that the addition of real numbers becomes the multiplication of the semiring).

Example 4.6.2. ([21, Table III]) Consider the following three-element binary structure $A(+,\cdot)$:

$+$	o	0	1
o	o	o	o
0	o	0	1
1	o	1	1

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

It is easy to check that $A=A(+,\cdot)$ is a bi-idempotent semiring possessing an additively absorbing element (namely o), an additively neutral element (namely 0), two multiplicatively right absorbing elements (namely o and 0), no multiplicatively absorbing element and a multiplicatively neutral element (namely 1). Moreover, the semigroup $A(\cdot)$ is linearly ordered by $o\leq 1\leq 0$ and we have $A=\mathrm{W}(A(\cdot,\leq))$. Finally, the semiring A is congruence-simple albeit none of the semigroups $A(+)$ and $A(\cdot)$ is so.

Proposition 4.7. ([7, 5.3]) *Let S be a congruence-simple commutative additively idempotent semiring without an additively absorbing element (cf. 4.3). Then there exists a subsemigroup A of $\mathbb{R}(+)$ such that $A\cap\mathbb{R}^+\neq\emptyset\neq A\cap\mathbb{R}^-$ and S is isomorphic to $\mathrm{W}(A(+,\leq))$ (see 4.6.1).*

5. Congruence-simple additively cancellative semirings

Theorem 5.1. *Let S be a non-trivial additively cancellative semiring. Then S is congruence-simple if and only if the following three conditions are satisfied:*

(1) *The ring $R=S-S$ of differences of S is simple (cf. 1.2);*

(2) *S is bi-ideal-simple (i.e., $S=S+SaS$ for every $a\in S$);*

(3) *S is additively archimedean (i.e., for all $a,b\in S$ there exist $c\in S$ and a positive integer n such that $b+c=na$).*

Proof. It is divided into four parts.

(i) If r is a congruence of S, then $I=\{a-b\ ;\ (a,b)\in r\}$ is an ideal of R and we have $I=0$ if and only if $r=\mathrm{id}_S$. Moreover, if $r=S\times S$, then $I=R$ and the converse is true, provided that S/r is additively cancellative. Thus id_S and $S\times S$ are the only congruences r of S such that S/r is cancellative if and only if the difference ring R is simple.

(ii) Define a relation s on S by $(a,b)\in s$ if and only if $a+x=mb$ and $b+y=na$ for some $x,y\in S$ and positive integers m,n. Then s is a congruence of S and $(a,2a)\in s$ for every $a\in S$. Since S is non-trivial and cancellative, we have $s\neq\mathrm{id}_S$.

(iii) Assume that S is congruence-simple. Then the condition (1) follows from (i), the condition (2) from 1.1 and the condition (3) from (ii).

(iv) Now, conversely, assume that the conditions (1), (2) and (3) are satisfied. If S is a ring, then $R=S$ and S is congruence-simple by (1) and 1.2. Consequently, we will assume that S is not a ring.

Let r be a congruence of S such that $(w, 2w) \in r$ for some $w \in S$. We claim that $r = S \times S$. To show this, denote by φ the natural projection of S onto $T = S/r$ and observe that (due to (3)) $\varphi(w)$ is the only idempotent of $T(+)$. Then $T\varphi(w) = \varphi(w) = \varphi(w)T$ and, by (2), $\varphi(w) + T = T$. From this, we conclude that $\varphi(w) = 0$ in T and that T is a ring. But then $r = S \times S$ by (1).

Let s be a congruence of S such that $s \neq S \times S$. Given $w \in S$, we have $(w, 2w) \notin s$ and we can consider a congruence t of S maximal with respect to $s \subseteq t$ and $(w, 2w) \notin t$. Then t is a maximal congruence of S and $P = S/t$ is a congruence-simple semiring whose additive semigroup possesses no idempotents. Applying 2.1, we see that P is additively cancellative and consequently $s = t = \mathrm{id}_S$ by (1) and (i). Thus S is congruence-simple. □

Proposition 5.2. *Let S be a non-trivial additively cancellative semiring satisfying 5.1 (1), (3) and such that S is finitely generated as a bi-ideal. Then S is congruence-simple if and only if $S = \{2a \ ; \ a \in S\} \cup \{2a + b \ ; \ a, b \in S\}$.*

Proof. The set $A = \{2a\} \cup \{2a + b\}$ is a bi-ideal of S, and hence $A = S$, provided that S is congruence-simple. Now, conversely, assume that $A = S$ and S is not congruence-simple. Then, according to 5.1 (and the proof of 5.1), S is not bi-ideal-simple and id_S, $S \times S$ are the only additively cancellative congruences of S. Furthermore, due to 2.3, S has at least one maximal congruence r. Clearly, the semiring $T = S/r$ inherits 5.1 (3) and 2.1 yields a contradiction. □

Proposition 5.3. *Let S be a non-trivial additively cancellative semiring satisfying 5.1 (1), (3) and let $w \in S$ be such that $w = w^2$. Then S is congruence-simple if and only if $S = S + SwS$ (e.g., $S + S = S$ and w is left or right multiplicatively neutral).*

Proof. Using [8, 8.12] we can proceed similarly as in the proof of 5.3. □

Theorem 5.4. *Let S be a congruence-simple additively cancellative semiring.*
(i) *If $0_S \in S$, then S is a ring.*
(ii) *If $1_S \in S$, then either S is a ring or S is commutative.*

Proof. (i) This assertion follows immediately from 5.1(3).

(ii) Assume that S is not a ring. By (i), $0 \notin S$. On the other hand, the unit element $1 = 1_S$ is also a unit element of the difference ring $R = S - S$ of S and we are going to show that R is a commutative ring (in fact, a field). For that purpose, we shall make use of a variation on a well known method developed by Goodearl and Handelman (see [10] for details and further references). The backgrounds of the mentioned method go back to Hölder and Hilbert (cf. [15] and [16]; but see also [1], [2], [4], [11], [19] and [22]).

The rest of the proof is divided into seven parts.

(a) Denote by $\mathbf{A}$ the set of subgroups A of the additive group $R(+)$ such that $1_R \in A$. A homomorphism $f : A(+) \to \mathbb{R}(+)$ ($\mathbb{R}$ being the field of real numbers) will be called positive if $f(a) \geq 0$ for every $a \in A \cap S$. Furthermore, such a homomorphism f will be called principal if for every positive homomorphism $g : A(+) \to \mathbb{R}(+)$ such that $g(a) \leq f(a)$ for every $a \in A \cap S$ there exists a non-negative real number r with $g = rf$.

(b) Put $A_0 = \mathbb{Z}1_R$ and define $f_0 : A_0 \to \mathbb{R}$ by $f_0(n1_R) = n$ for every $n \in \mathbb{Z}$. Then $f_0(1_R) = 1$ and f_0 is an injective principal positive homomorphism of $A_0(+)$ into $\mathbb{R}(+)$.

(c) Let A_i, $i \in I$, be a non-empty chain of subgroups from $\mathbf{A}$ and let $f_i : A_i(+) \to \mathbb{R}(+)$ be principal positive homomorphisms such that $f_j = f_i|A_j$ whenever $A_j \subseteq A_i$. Then $A = \bigcup_I A_i$ is from $\mathbf{A}$ and $f = \bigcup_I f_i$ is a principal positive homomorphism of $A(+)$ into $\mathbb{R}(+)$.

(d) Let $A \in \mathbf{A}$ and let $f : A(+) \to \mathbb{R}(+)$ be a principal positive homomorphism. Now, take $w \in R$ and put $r = \sup\{n^{-1}f(a)\ ;\ a \in A, n \geq 1, nw - a \in S \cup \{0\}\}$ and $B = A + \mathbb{Z}w$. Further, assume for a moment that $b + mw \in S \cup \{0\}$ for some $b \in A$ and $m \in \mathbb{Z}$. If $0 < m$, then $m^{-1}(-f(b)) \leq r$ and $0 \leq f(b) + mr$. If $m < 0$, then $r \leq (-m)^{-1}f(b)$ and, again, $0 \leq f(b) + mr$. Now, we see that we can define a positive homomorphism $g : B(+) \to \mathbb{R}(+)$ by $g(b + mw) = f(b) + mr$, $b \in A$, $m \in \mathbb{Z}$. It remains to check that g is principal.

Let $k : B(+) \to \mathbb{R}(+)$ be a positive homomorphism such that $k(c) \leq g(c)$ for every $c \in B \cap S$. Since f is principal, $k|A = sf$ for some $s \in \mathbb{R}$, $s \geq 0$. If $rs < k(w)$, then there exist $b \in A$ and $m \geq 1$ such that $mw - b \in S \cup \{0\}$ and $r - m^{-1}f(b) < k(w) - rs$. We have $k(mw - b) \leq g(mw - b)$, and therefore $k(w) - rs \leq k(w) - sm^{-1}f(b) \leq r - m^{-1}f(b) < k(w) - rs$, a contradiction. On the other hand, if $nw - a \in S \cup \{0\}$, $a \in A$, $n \geq 1$, then $0 \leq k(nw - a) = nk(w) - sf(a)$, $n^{-1}sf(a) \leq k(w)$ and $rs \leq k(w)$. Thus $k(w) = rs$ and $k = sg$.

(e) Denote by $\mathbf{M}$ the set of ordered pairs (A, f), where $A \in \mathbf{A}$ and $f : A(+) \to \mathbb{R}(+)$ is a principal positive homomorphism such that $f(1_R) = 1$. The set $\mathbf{M}$ is non-empty (by (a)) and it is ordered in obvious way. Now, if (A, f) is maximal in $\mathbf{M}$ (by (c)), then it follows from (d) that $A = R$.

(f) Let $f : R(+) \to \mathbb{R}(+)$ be a principal positive homomorphism such that $f(1_R) = 1$. We are going to show that f is a ring homomorphism.

For every $a \in S \cup \{0\}$, define a mapping $g_a : R \to \mathbb{R}$ by $g_a(x) = f(ax)$, $x \in R$. Then $g_a : R(+) \to \mathbb{R}(+)$ is a positive homomorphism and there is $n_a \geq 1$ such that $n_a 1_R - a \in S$ and $g_a(b) = f(ab) \leq f(n_a b) = n_a f(b)$, $n_a^{-1} g_a(b) \leq f(b)$ for every $b \in S \cup \{0\}$. Since f is principal, $g_a = \rho(a)f$ for some $\rho(a) \in \mathbb{R}$, $\rho(a) \geq 0$.

If $a, b \in S \cup \{0\}$, then $\rho(a + b) = \rho(a + b)f(1_R) = g_{a+b}(1_R) = f((a + b)1_R) = f(a) + f(b) = g_a(1_R) + g_b(1_R) = \rho(a)f(1_R) + \rho(b)f(1_R) = \rho(a) + \rho(b)$. Similarly, $\rho(ab) = \rho(ab)f(1_R) = g_{ab}(1_R) = f(ab) = g_a(b) = \rho(a)f(b) = \rho(a)f(b1_R) = \rho(a)\rho(b)f(1_R) = \rho(a)\rho(b)$.

We have checked that ρ is a homomorphism of the semiring $S \cup \{0\}$ into the field $\mathbb{R}$ such that $\rho(0) = 0$ and $\rho(1_S) = 1$. Now, $R = S - S$ and ρ extends (uniquely) to a ring homomorphism (denote it again by ρ) of R into $\mathbb{R}$. If $a \in S$, then $f(a) = f(a1_R) = g_a(1_R) = \rho(a)f(1_R) = \rho(a)$. Thus $\rho = f$.

(g) According to (f), there exists at least one ring homomorphism $f : R \to \mathbb{R}$ such that $f(1_R) = 1$ and $f(a) \geq 0$ for every $a \in S$. Since R is a simple ring, we have $\mathrm{Ker}(f) = 0$, f is injective and $f(a) > 0$ for every $a \in S$. □

Remark 5.5. We have proven in 5.4 that every congruence-simple additively cancellative semiring that contains a unit and is not a ring is isomorphic to a subsemiring of the semiring $\mathbb{R}^+$ of positive real numbers. According to [7, 8.5], every congruence-simple additively cancellative commutative semiring that is not a ring is isomorphic to a subsemiring of $\mathbb{R}^+$.

Remark 5.6. (cf. 5.3 and 5.5) Let S be a subsemiring of $\mathbb{R}^+$ such that the multiplicative semigroup $S(\cdot)$ is a group.

(i) According to [7, 8.3], S is congruence-simple if and only if for every $a \in S$, $a \neq 1$, there exist $b, c \in S$ and a positive integer n such that $a + b = n$ and $(a-1)(1-c) \in S$.

(ii) According to [18, Satz 2], S is congruence-simple, provided that every element from S is algebraic.

(iii) Let $\alpha \in \mathbb{R}^+$ be a transcendental number and $S = \{a_1^2 + ... + a_n^2\ ;\ n \geq 1, a_i \in \mathbb{Q}(\alpha), a_i \neq 0\}$. Then S is a subsemiring of $\mathbb{R}^+$, $S(\cdot)$ is a group, $\alpha^{-2} \in S$ and the set $\alpha^{-2} + S$ contains no positive integers. That is, $S(+)$ is not archimedean and S is not congruence-simple.

Remark 5.7. (cf. 5.5 and [20, 5.7]) Let S be a congruence-simple subsemiring of $\mathbb{R}^+$ such that $n^{-1} \in S$ for at least one integer $n \geq 2$. By [7, 9.7], the multiplicative semigroup $S(\cdot)$ is a group (and hence $\mathbb{Q}^+ \subseteq S$).

Example 5.8. Let $S = \mathrm{M}_n(\mathbb{Q}^+)$, $n \geq 2$, $\mathbb{Q}^+$ being the semiring of positive rationals. Then S is additively cancellative and not commutative. Moreover, it is easy to check that S satisfies the conditions 5.1(1),(2),(3) and consequently, S is congruence-simple. Of course, S is not a ring and S does not contain a unit element (and S is not isomorphic to any subsemiring of $\mathbb{R}$ either).

6. Congruence-simple additively zeropotent semirings with $S = S + S$

Remark 6.1. Let S be an additively zeropotent semiring (i.e., $o_S \in S$ and $2S = o_S$). We define a relation $\leq$ on S by $a \leq b$ iff $a \in (S + b) \cup \{b\}$. One checks easily that the relation is an order compatible with the two operations defined on S and that the bi-absorbing element o_S is a smallest element of $S(\leq)$. Now, if $S = S + S$ and $|S| \geq 2$, then (see [8]):

(i) S is infinite.

(ii) The ordered set $S(\leq)$ has no maximal elements.

(iii) o_S is the only additively and/or multiplicatively idempotent element of S.

(iv) If $a \in S$ is not nilpotent, then the elements a^i, $i \geq 1$, are pair-wise incomparable in $S(\leq)$.

(v) S is not a nil-semiring.

(vi) S is not commutative.

Remark 6.2. Let S be a congruence-simple additively zeropotent semiring such that S is not additively constant (see 2.1). Then S is non-trivial and $S = S + S$ (see 6.1). So far, no example of such a semiring is known (at least to the authors of the present brief note). Anyway, 1.3 could be of some help.

7. Congruence-simple additively constant semirings

Lemma 7.1. *Let S be an additively constant semiring. A relation r is a congruence of the semiring S if and only if it is a congruence of the multiplicative semigroup $S(\cdot)$.*

Proof. Obvious. □

Corollary 7.2. *An additively constant semiring S is congruence-simple if and only if so is the multiplicative semigroup $S(\cdot)$.*

Construction 7.3. Let S be a multiplicative semigroup containing an absorbing element o_S. Now, define an addition on S by $a + b = o$ for all $a, b \in S$. Then $\mathrm{U}(S(\cdot)) = S(+, \cdot)$ becomes an additively constant semiring. This semiring is congruence-simple if and only if so is the semigroup $S(\cdot)$.

Remark 7.4. All finite congruence-simple semigroups with absorbing element are known (see e.g. [17, 3.7.1]).

8. Congruence-simple semirings of some classes

Proposition 8.1. ([21]) *Let S be a finite congruence-simple semiring. Then just one of the following four cases takes place:*

(1) S is additively idempotent and contains an additively absorbing element;
(2) S is a zero multiplication ring of finite prime order;
(3) S is (a copy of) a matrix ring over a finite field;
(4) S is additively constant (see 7.3 and 7.4).

Proof. If $S = \{a_1, ..., a_m\}$ is additively idempotent, then the sum $a_1 + ... + a_m$ is the additively absorbing element. Now, with regard to 2.1 and 6.1 (i), we may assume that S is additively cancellative. Then S is a finite simple ring (1.2) and it follows easily that $pS = 0$ for a prime $p \geq 2$. Setting $R = S \times \mathbb{Z}_p$ and defining $(a, r) + (b, s) = (a + b, r + s)$, $(a, r)(b, s) = (ab + rb + sa, rs)$, we get a finite ring R containing S as an ideal and such that $pR = 0$ and $1_R = (0, 1) \in R$ (R is a factor of the Dorroh extension of S). If $S \subseteq \mathrm{J}(R)$, then S is nilpotent and (2) is true. If $S \not\subseteq \mathrm{J}(R)$, then $S \cap \mathrm{J}(R) = 0$ and S embeds into $T = R/\mathrm{J}(R)$. The latter ring is a direct sum of matrix rings over finite fields, and hence S occurrs as a non-zero ideal of $\mathrm{M}_n(F)$ for a finite field F. The matrix ring is simple, and so $S \simeq \mathrm{M}_n(F)$. □

Proposition 8.2. *Let S be a congruence-simple semiring containing an additively neutral element 0. Then either S is additively idempotent (and $a + b \neq 0$ for all $a, b \in S$, $a \neq 0$) or S is a (simple) ring (see 1.2).*

Proof. Combine 2.1 and 5.4 (i). □

Proposition 8.3. *Let S be a congruence-simple semiring containing a multiplicatively neutral element. Then just one of the following five cases is true:*

(1) S is additively idempotent;
(2) S is isomorphic to a subsemiring of $\mathbb{R}^+$;
(3) S is a (simple) ring with unit;
(4) S is infinite and additively constant;
(5) $S \simeq Z_2$.

Proof. Combine 2.1, 5.4 (ii), 5.5, 6.1 (iii) and 7.2. □

Remark 8.4. Combining 8.1 and 8.2 (8.3), we get a classification of finite congruence-simple semirings possessing an additively (multiplicatively) neutral element.

Proposition 8.5. *Let S be a congruence-simple semiring containing an element w such that the set $T = S \setminus \{w\}$ is a subgroup of the multiplicative semigroup $S(\cdot)$. Then just one of the following three cases holds:*

(1) S is isomorphic to one of the two-element semirings Z_1, ..., Z_5, Z_7, Z_9 and Z_{10};

(2) S is additively idempotent, $w = o_S$ is a bi-absorbing element of S and S is constructed in the way described in 4.4 (if S is finite, then $S = \mathrm{V}(S(\cdot))$ - see 4.1);

(3) S is a division ring (if S is finite, then S is a field).

Proof. We may assume that $|S| \geq 3$. Now, it follows from 1.6 and 2.2, that w is multiplicatively absorbing or multiplicatively neutral.

Firstly, let w be multiplicatively absorbing. If w is not bi-absorbing, then S is a division ring by 1.7 (i), and therefore we assume that $w = o_S$ is bi-absorbing. The unit element of the group $T(\cdot)$ is a multiplicatively neutral element of S, and hence 2.1 (3) is not true (6.1 (iii)). If S is additively constant, then $(T \times T) \cup \mathrm{id}_S$ is a congruence of S and $|S| = 2$, a contradiction. Thus, in view of 2.1, S is additively idempotent.

Next, let w be multiplicatively neutral. Then 1.7 (ii) yields $|S| = 2$, a contradiction. □

Proposition 8.6. *Let S be a congruence-simple semiring such that the multiplicative semigroup $S(\cdot)$ is a group. Then S is infinite and either S is additively idempotent (see 4.5) or S is isomorphic to a subsemiring of $\mathbb{R}^+$ (see 5.6).*

Proof. The automorphism group of $S(+)$ operates transitively on S, and hence S is infinite and S contains no additively absorbing and no additively neutral element. Moreover, by 2.1, S is either additively idempotent or additively cancellative. Of course, S contains a multiplicatively neutral element and no multiplicatively absorbing element. The rest is clear from 8.2. □

Lemma 8.7. *Let S be a congruence-simple semiring such that S is not a ring. Define a relation $\leq$ on S by $a \leq b$ if and only if $a \in (S + b) \cup \{b\}$. Then:*

(i) The relation $\leq$ is an ordering compatible with both the addition and the multiplication of the semiring S.

(ii) The ordering $\leq$ is downwards directed (we have $a + b \leq a$ and $a + b \leq b$).

(iii) If $o_S \in S$, then o_S is the smallest element of $S(\leq)$.

(iv) If $0_S \in S$, then 0_S is the greatest element of $S(\leq)$.

(v) The ordering $\leq$ is linear if and only if the semiring S is additively semisubtractive (i.e., for all $a, b \in S$, $a \neq b$, there is $c \in S$ with $a + c = b$ or $b + c = a$).

Proof. Clearly, the relation $\leq$ is reflexive, transitive and compatible. Let $a, b, c, d \in S$ be such that $a + c = b$ and $b + d = a$. Then $a + e = a$ and $b + e = b$, where $e = c + d$.

If S is additively idempotent, then $a = b + d = b + b + d = b + a = a + c + a = a + c = b$.

If S is additively cancellative, then $x + a = x + a + e$ implies $x = x + e$ for every $x \in S$. Now, $e = 0_S$ and S is a ring by 5.4 (i), a contradiction.

If S is additively zeropotent, then $a = a + e = a + 2e = o$ and, similarly, $b = o$.

The rest is clear from 2.1. □

Proposition 8.8. *Let S be a congruence-simple semiring whose additive semigroup is semisubtractive (see 8.7 (v)). Then just one of the following four cases holds:*

(1) S is isomorphic to one of the two-element semirings Z_1 and Z_2;

(2) S is additively idempotent and $S(+)$ is a chain (see 4.6);

(3) S is a simple ring (see 1.2);

(4) There exists a subfield F of the field $\mathbb{R}$ of real numbers such that S is isomorphic to the semiring $F \cap \mathbb{R}^+$ (then $S(\cdot)$ is a group).

Proof. In view of 2.1, assume that $|S| \geq 3$ and that S is not additively idempotent. If S is additively zeropotent and $a, b \in S$, $a \neq b$, then there is $c \in S$ such that $a + c = b$ or $b + c = a$. In both cases, $a + b = o_S$, and hence S is additively constant and it follows easily that $|S| = 2$, a contradiction. Consequently, we may assume that S is additively cancellative, but that S is not a ring (5.4 (i)).

Let R be the difference ring of S. Now, (4) follows from 5.1 and the well known Hölder Theorem (see [1], [2], [4], [16], [19] and [22]). □

Corollary 8.9. *Let S be a finite congruence-simple semiring whose additive semigroup is semisubtractive. Then just one of the following four cases holds:*
(1) S is isomorphic to one of the two-element semirings Z_1 and Z_2;
(2) S is additively idempotent and $S(+)$ is a finite chain;
(3) S is a zero multiplication ring of finite prime order;
(4) S is a matrix ring over a finite field.

Acknowledgement. The authors are grateful to anonymous referee for correcting several inaccuracies in the original version.

References

[1] R. Baer, *Zür Topologie der Gruppen,* Journal für die reine und angew. Math. 160 (1929), 208-226.
[2] H. Cartan, *Une théorème sur les groupes ordonnés,* Bull. Sci. Math. 63 (1939), 201-205.
[3] C. G. Chechata, *An algebraically simple ordered group,* Proc. London Math. Soc. 2 (1952), 183-197.
[4] J. V. Chion, *Archimedovski uporjadočennyje kol'ca,* Uspechi mat. nauk 9 (1954), 237-242.
[5] V. Dlab, *On a family of simple ordered groups,* J. Austral. Math. Soc. 8 (1968), 591-608.
[6] R. Eilhauer, *Zur Theorie der Halbkörper, I,* Acta Math. Acad. Sci. Hungar. 19 (1968), 23-45.
[7] R. El Bashir, J. Hurt, A. Jančařík and T. Kepka, *Simple commutative semirings,* J. Algebra 236 (2001), 277-306.
[8] V. Flaška, T. Kepka and J. Šaroch, *Bi-ideal-simple semirings,* Comment. Math. Univ. Carolinae 46 (2005), 391-397.
[9] J. Golan, *The Theory of Semirings with Applications in Math. and Theor. Computer Science,* Pitman Monographs and Surveys in Pure and Appl. Math., Vol. 54, Longman, Harlow, 1992.
[10] K. R. Goodearl, *Partially ordered groups with interpolation,* Mathem. Surveys and Monographs 20, Amer. Math. Soc., Providence 1986.
[11] D. Handelman, *Positive polynomials and product type actions of compact groups,* Mem. Amer. Math. Soc. 320 (1985).
[12] U. Hebisch and H. J. Weinert, *Halbringe - Algebraische Theorie und Anwendungen in der Informatik,* Teubner, Stuttgart, 1993.
[13] U. Hebisch and H. J. Weinert, *Semirings and semifields,* in: Handbook of Algebra, vol. 1, Elsevier Science B. V., 1996, 425-462.
[14] G. Higman, *On infinite simple permutation groups,* Publ. Math. Debrecen 3 (1955), 221-226.
[15] D. Hilbert, *Grundlagen der Geometrie.* Teubner, Leipzig/Berlin, 1930.
[16] O. Hölder, *Die Axiome der Quantität und die Lehre vom Mass,* Berichte über die Verhandlungen der Königlich Sächsischen Gesellschaft der Wissenschaften zu Leipzig, Mathematisch-Physische Classe 53 (1901), 1-64.
[17] J. Howie, *Fundamentals of Semigroup Theory,* Oxford University Press, 1995.
[18] H. Koch, *Über Halbkörper, die in algebraischen Zahlkörpern enthalten sind,* Acta Math. Acad. Sci. Hungar. 15 (1964), 439-444.
[19] F. Loonstra, *Ordered groups,* Proc. Nederl. Akad. Wetensch. 49 (1945), 41-66.

[20] S. S. Mitchell and P. B. Fenoglio, *Congruence-free commutative semirings,* Semigroup Forum 37 (1988), 79-91.
[21] Ch. Monico, *On finite congruence-simple semirings,* J. Algebra 271 (2004), 846-854.
[22] G. Tallini, *Sui sistemi a doppia composizione ordinati archimedei,* Atti Accad. Nat. Lincei Rend. Cl. Fis. Mat. Nat. 18 (1955), 367-373.

MFF UK, Sokolovská 83, Praha 8, 186 75, Czech Republic
bashir@karlin.mff.cuni.cz kepka@karlin.mff.cuni.cz