Journal of Algebra **236,** 277–306 (2001)
doi:10.1006/jabr.2000.8483, available online at http://www.idealibrary.com on IDEAL®

Simple Commutative Semirings

R. El Bashir, J. Hurt, A. Jančařík, and T. Kepka[1]

Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic
E-mail: bashir@karlin.mff.cuni.cz; hurt@karlin.mff.cuni.cz; jancarik@karlin.mff.cuni.cz; kepka@karlin.mff.cuni.cz

Communicated by Kent R. Fuller

Received February 1, 2000

Key Words: commutative semiring; cancellative semiring; parasemifield; semifield.

0. INTRODUCTION

The notion of a semiring (i.e., a universal algebra with two associative binary operations, where one of them distributes over the other) was introduced by Vandiver [33] in 1934. Needless to say, semirings found their full place in mathematics long before that year (e.g., the semirings of positive elements in ordered rings) and even more so after (e.g., various applications in theoretical computer science and algorithm theory). However, the reader is referred to [11, 12, 16, and 17] for background, basic, and more advanced properties of, and comments, historical remarks, and further references on semirings.

Congruence-simple algebras (i.e., those possessing just two congruence relations) serve a basic construction material for any algebraic structure. In spite of the fact and in contrast to the enormous and opulent supply of

[1] While working in this paper, the first and fourth authors were supported by the grant agency of Charles University, Grant 3051-10/716, and the second author was supported by the grant agency of the Czech Republic, Grant 201/97/1176. The first author was also supported by the grant agency of the Czech Republic, POSTDOC Grant #201/98/P247.
The authors were also supported by the institutional grant CEZ: J13/98: 113 200 007.

0021-8693/01 $35.00

information on worldwide popular simple groups and rings, not much is known on congruence-simple semigroups and almost nothing on such semirings. We mention only that the study of congruence-simple commutative semirings with unit was initiated in [26] (see also [12]) and that some results on congruence-simple semifields was achieved in [21].

The aim of the present paper is to classify the congruence-simple commutative semirings and to relate them with better known concepts (for instance, ordered rings with order units). To that purpose, the paper is divided into 14 parts and the promised classification is summarized in the 10th section. Additionally, for a better understanding, some basic information on ideal-simple commutative semirings is included.

1. PRELIMINARIES

A commutative semiring is a non-empty set equipped with two associative and commutative binary operations (usually denoted as addition and multiplication) such that the multiplication is distributive over the addition. (Note that the existence of any neutral and/or absorbing element is not assumed *a priori*.) In the following we shall be handling commutative semirings only, and hence the word *semiring* will always mean a *commutative semiring*.

Let S be a semiring. A (binary) relation $r \subseteq S \times S$ is a congruence of S if r is an equivalence and $(a + c, b + c) \in r$, $(ac, bc) \in r$ for all $(a, b) \in r$ and $c \in S$. A non-empty subset I of S is an *ideal* or *bi-ideal* of S if $SI \subseteq I$ and $I + I \subseteq I$ or $S + I \subseteq I$, respectively. The semiring S will be called *congruence-simple* (or cg-simple, for short) if S is non-trivial and id_S, $S \times S$ are the only congruences of S; and *ideal-simple* (id-simple for short), or *bi-ideal-simple* if S is non-trivial and $I = S$ whenever I is an ideal or bi-ideal of S such that I contains at least two elements, respectively. If I is a bi-ideal of S, then $(I \times I) \cup \mathrm{id}_S$ is a congruence of S and consequently S is bi-ideal-simple provided that S is cg-simple or id-simple. Note that a (non-trivial commutative) ring is congruence/ideal-simple (as a semiring or a ring) if and only if it is a field or a zero multiplication ring of finite prime order. Note also that every two-element semiring is both congruence- and ideal-simple and that there exist (up to isomorphism) just eight two-element semirings (see the next section).

A semiring S is said to be *additively* (resp., *multiplicatively*) *idempotent/cancellative* if so is the additive (resp., multiplicative) semigroup $S(+)$ (resp., $S(\cdot)$). These semirings will also be called *ai/ac-semirings* (or *mi/mc-semirings*).

2. TWO-ELEMENT COMMUTATIVE SEMIRINGS

Z_1

$+$	0	1
0	0	0
1	0	0

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

Z_2

$+$	0	1
0	0	0
1	0	0

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

Z_3

$+$	0	1
0	0	0
1	0	1

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

Z_4

$+$	0	1
0	0	0
1	0	1

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

Z_5

$+$	0	1
0	0	0
1	0	1

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

Z_6

$+$	0	1
0	0	0
1	0	1

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

Z_7

$+$	0	1
0	0	1
1	1	0

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

Z_8

$+$	0	1
0	0	1
1	1	0

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

3. CONGRUENCE-SIMPLE COMMUTATIVE SEMIRINGS—BASIC CLASSIFICATION

3.1. THEOREM. *Let S be a congruence-simple semiring. Then just one of the following three cases takes place*:

(1) *S is a two-element semiring isomorphic either to Z_1 or Z_2,*

(2) *S is additively idempotent.*

(3) *S is additively cancellative.*

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 the semiring S and we have either $r = \mathrm{id}_S$ or $r = S \times S$.

Let $r = \mathrm{id}_S$. The mapping $x \mapsto 2x$ is an injective transformation of S and we shall define a relation s on S by $(x, y) \in s$ if and only if there exist a non-negative integer i and elements $u, v \in S \cup \{0\}$ such that $2^i x = y + u$ and $2^i y = x + v$. Again, s is a congruence of S and $(x, 2x) \in s$ for every $s \in S$. Consequently, if $s = \mathrm{id}_S$, then $S(+)$ is idempotent and hence we shall assume that $s = S \times S$ and $a + b = a + c$ for some $a, b, c \in S$. There exist $i \geq 0$ and $w \in S \cup \{0\}$ such that $2^i b = a + w$ and we have $b + 2^i b = b + a + w = c + a + w = c + 2^i b$. Then $2b = b + c$ for $i = 0$ and, if $i \geq 1$, then $2(b + 2^{i-1}b) = 2(c + 2^{i-1}b)$, $b + 2^{i-b} = c + 2^{i-1}b$, and $2b = b + c$ by induction. Quite similarly, $b + c = 2c$, and so $2b = 2c$ and, finally, $b = c$. We have proved that $S(+)$ is cancellative.

Now let $r = S \times S$. Then there is an $o \in S$ such that $2x = o$ for every $x \in S$. Similarly as above, define a congruence t of S by $(x, y) \in t$ if and only if $3x = 3y$. If $t = \mathrm{id}_S$ and $a + b = a + c$, then $x \mapsto 3x$ is injective and the equalities $3b = b + o = b + a + a = c + a + a = c + o = 3c$ imply $b = c$ (hence $S(+)$ is cancellative). Therefore, assuming that $t = S \times S$, i.e., $x + o = o$ for every $x \in S$. We have to consider the following four cases:

Let $S + S = S$ and $SS \neq o$. Then there are $a, b, c, d \in S$ such that $a + b = c$ and $cd \neq o$. Since $xo = x(o + o) = xo + xo = o$ for every $x \in S$, we know that all the elements a, b, c, d are different from o. Put $I = \{x; x = cu + v, u \in S, v \in S \cup \{0\}\}$. Then I is a bi-ideal of S and $o, cd \in I$. Thus $I = S$ and, in particular, $a = cu_1 + v_1$ and $b = cu_2 + v_2$ for suitable $u_1, u_2 \in S$ and $v_1, v_2 \in S \cup \{0\}$. But then $a = (a + b)u_1 + v_1 = au_1 + v_1 + v_2u_1 + cu_2u_1$, $b = (a + b)u_2 + v_2 = bu_2 + v_2 + v_1u_2 + cu_1u_2$, and $o \neq c = a + b = au_1 + v_1 + v_2u_1 + bu_2 + v_2 + v_1u_2 + 2cu_1u_2 = o$, since $2cu_1u_2 = o$, a contradiction.

Let $S + S \neq o = SS$. We have $a + b = c \neq o$ for some $a, b, c \in S$ and the relation p defined on S by $(x, y) \in p$ if and only if $a + x = a + y$ is a congruence of S. Of course, $(a, o) \in p$, $p \neq \mathrm{id}_S$, $p = S \times S$, $(b, o) \in p$, and $o \neq c = a + b = a + o = o$, a contradiction.

Let $S + S = o \neq SS$. Put $J = \{x \in S; xS = o\}$. Then $J \neq S$ and, since J is a bi-ideal of S, we must have $J = \{o\}$. Put $T = S \setminus \{o\}$, and, for every $a \in T$, define a relation h_a on S by $(x, y) \in h_a$ if and only if $ax = ay$. Then h_a is a congruence of S, $(b, o) \notin h_a$, for at least one $b \in T$ and consequently $h_a = \mathrm{id}_S$. Thus $TT \subseteq T$ and the relation $q_T = (T \times T) \cup \mathrm{id}_S$ is a congruence of S. Since $q_T \neq S \times S$, we have $q_T = \mathrm{id}_S$, $\mathrm{card}(T) = 1$, and $S \cong Z_2$.

Let $S + S = o = SS$. Then every equivalence defined on S is a congruence of S, and therefore $|S| = 2$ and $S \cong Z_1$. ∎

3.2. EXAMPLE (cf. [26, 4.1]). Let G be an abelian group (denoted multiplicatively), $o \notin G$, and $V(G) = G \cup \{o\}$. Put $x + y = o$, $x + x = x$, and $xo = o = ox$ for all $x, y \in V(G)$, $x \neq y$. The $V(G)$ becomes a (commutative) ai-semiring (possessing a unit) and o is a smallest (alias absorbing) element of the semilattice $V(G)(+)$. Moreover, it is easy to see that $V(G)$ is both congruence- and ideal-simple. Note also that $V(G)$ is a finitely generated semiring if and only if the group G is finitely generated and that $V(G_1) \cong V(G_2)$ if and only if $G_1 \cong G_2$.

3.3. THEOREM (cf. [26, 4.7]). *Let S be a congruence-simple additively idempotent semiring. Then just one of the following three cases takes place*:

(α) *S is isomorphic to one of the two-element semirings Z_3, Z_4, Z_5.*

(β) *The additive semilattice $S(+)$ possesses a smallest element o (i.e., $x + o = o$ for every $x \in S$), So $= o$, $G = S \setminus \{o\}$ is an (abelian) subgroup of*

the multiplicative semigroup $S(\cdot)$, and the semiring S is (isomorphic to) the semiring $V(G)$ (see 3.2).

(γ) *The semiring S is multiplicatively cancellative.*

Proof. Put $A = \{x \in S;\ \mathrm{card}(Sx) = 1\}$. If $a \in S \setminus A$ and if r_a is defined by $(x, y) \in r_a$ if and only if $ax = ay$, then r_a is a congruence of S, $r_a \neq S \times S$, $r_a = \mathrm{id}_S$, and the map $x \mapsto ax$ is an injective transformation of S. Now, if $A = \emptyset$, then (γ) is true, hence assume that $A \neq \emptyset$.

One sees easily that there exists an element $w \in S$ such that $SA = w = Sw$ and the set $S + w$ is a bi-ideal of S. If $S + w = S$, then $w = 0$ is a neutral element of $S(+)$, $(T \times T) \cup \mathrm{id}_S$ is a congruence of S, where $T = S \setminus \{0\}$, and we have $|T| = 1$, $|S| = 2$, an either $S \cong Z_4$ or $S \cong Z_5$. Hence, assume that $S + w = w$ and $w = o$ is a smallest element of $S(+)$.

Now, define a relation s on S by $(x, y) \in s$ if and only if $\{z_1 \in S;\ ax + z_1 = o\} = \{z_2 \in S;\ ay + z_2 = o\}$ for every $a \in S$. Then s is a congruence of S and we consider first the case $s = S \times S$. We have $(x, o) \in s$ for every $x \in S$ and it follows that $uv + z = o$ for all $u, v, z \in S$. In particular, $uv = uv + uv = o$, i.e., $SS = o$ and $A = S$. If $a \in S \setminus \{o\}$, then $S + a$ is a bi-ideal of S, a, $o \in S + a$, hence $S + a = S$, a is a neutral element of $S(+)$, $|S \setminus \{o\}| = 1$ and $S \cong Z_3$.

Next, assume that $s = \mathrm{id}_S$. Then $A \neq S$ and, if $z \in S \setminus A$ and $v \in A$, then $zv = o = zo$ implies $v = o$. This means that $A = \{o\}$ and that $G = S \setminus \{o\}$ is a subsemigroup of $S(\cdot)$. Clearly, G is a cancellative semigroup.

Now, let $a, b \in S$, $a \neq b$. We are going to show that $a + b = o$. Proceeding by contradiction, assume that $a + b = c \neq o$. Since $a \neq b$, we may also assume that $c \neq a$. Then $(a, c) \notin s = \mathrm{id}_S$ and there exist $d, e \in S$ such that $dc + e = o \neq da + e$; we have $d \neq o$ and $dc \neq o$. Further, denote by B the set of $x \in S$ such that $x + vdc = x$ for some $v \in S \cup \{1\}$. Then $o, dc \in B$, B is a bi-ideal of S, $B = S$, $da \in B$, and, finally, $da + wdc = da$ for some $w \in S \cup \{1\}$ (in fact, $da + dc = dc \neq da$, and so $w \in S$). Quite similarly, $da + u(da + e) = da$ for some $u \in S \cup \{1\}$. Now we have

$$
\begin{aligned}
da + uda &= da + u(da + e) + uda \\
&= da + uda + ue = da + u(da + e) = da, \\
da + wudc &= da = uda + uwdc = da + u(da + wdc) \\
&= da + uda = da, \\
wdc + wda &= wda + wdb + wda = wda + wdb = wdc, \\
wda &= wda + wuda + wue, \\
da + wue &= du + wdc + wue = wue + da + wdc + wda \\
&= wue + da + wdc + wda + wuda + wue \\
&= da + wdc + w(da + uda + ue) \\
&= da + wdc + wda = da + wdc = da.
\end{aligned}
$$

Finally,

$$o \neq da = da + da = da + wudc + da + wue = da + wu(dc + e)$$
$$= da + wuo = da + o = o,$$

a contradiction.

We have proved that $a + b = o$ for all $a, b \in S$, $a \neq b$. From this, it follows easily that Sa is a bi-ideal of S for every $a \in S$. If $a \in G$, then $|Sa| \geq 2$, and therefore $Sa = S$. Now, it is easy to conclude that $G(\cdot)$ is a group and $S \cong V(G)$. ∎

3.4. THEOREM. *Let S be a congruence-simple additively cancellative semiring. Then just one of the following three cases takes place*:

(α) *S is a zero-multiplication ring of finite prime order*;

(β) *S is a field*;

(γ) *The semiring S is multiplicatively cancellative and the additive semigroup $S(+)$ possesses no neutral element.*

Proof. First, assume that there exists a neutral element $0 \in S$ for the additive semigroup $S(+)$, denote by M the set of invertible elements of $S(+)$, and define a relation r on S by $(x, y) \in r$ if and only if $y = x + u$ for some $u \in M$. Since $S(+)$ is cancellative, we have $S0 = 0$, $SM \subseteq M$, and it follows easily that r is a congruence of S. If $r = S \times S$, then $M = S$, S is a ring, S is ideal-simple, and it is clear that either (α) or (β) is true. Now, let $r = \mathrm{id}_S$. Then $M = 0$ and we put $q = ((S \setminus \{0\}) \times (S \setminus \{0\})) \cup \mathrm{id}_S$. For every $a \in S$, the relation r_a defined by $(x, y) \in r_a$ if and only if $ax = ay$ is a congruence of S, $Sa = 0$ if $r_a = S \times S$, and $(S \setminus \{0\})a \neq 0$ if $r_a = \mathrm{id}_S$. Using these observations, we deduce easily that q is a congruence of S. But then $q = \mathrm{id}_S$, $|S| = 2$, and either $S \cong Z_7$ or $S \cong Z_8$.

Now, assume that $0 \notin S$ and put $A = \{x \in S; |Sx| = 1\}$. Proceeding in a manner similar to the proof of 3.3, we show that $A \neq \emptyset$ and that $S(\cdot)$ is cancellative. ∎

4. ADDITIVELY/MULTIPLICATIVELY CANCELLATIVE COMMUTATIVE SEMIRINGS—BASIC OBSERVATIONS

The results of this section are of auxiliary character; all are fairly basic and some of them may be considered more or less folklore. We shall not attribute them to any particular source.

By a *parasemifield* we will mean a non-trivial (commutative) semiring S such that the multiplicative semigroup $S(\cdot)$ is an (abelian) group.

4.1. PROPOSITION (The Parasemifield of Fractions). *Let S be a non-trivial mc-semiring. The there exists a parasemifield P $(= P(S))$ such that the following conditions are satisfied*:

(i) *S is a subsemiring of P and $P = \{ab^{-1}; a, b \in S\}$.*

(ii) *P is additively cancellative if and only if S is.*

(iii) *P is additively idempotent if and only if S is.*

(iv) *If S is congruence-simple, then P is.*

(v) *P is ideal-simple (in fact, P does not possess any proper ideal).*

Proof. The proof is standard and easy. ∎

4.2. PROPOSITION (The Ring of Differences). *Let S be a non-trivial ac-semiring. Then there exists a (commutative) ring R $(= R(S))$ such that the following conditions are satisfied*:

(i) *S is a subsemiring of R and $R = \{a - b; a, b \in S\}$.*

(ii) *R is a ring without zero divisors if and only if $ac + bd \neq ad + bc$ for all $a, b, c, d \in S$; $a \neq b$; $c \neq d$.*

(iii) *R possesses a unit if and only if there exist $a, b \in S$ such that $ax + by + y = ay + bx + x$ for all $x, y \in S$.*

(iv) *If S possesses a unit, then R does also.*

(v) *R is a field if and only if for all $a, b, c, d \in S$; $a \neq b$; there exist $x, y \in S$ such that $ax + by + c = ay + bx + d$.*

Proof. The proof is standard and easy. ∎

A non-trivial additively cancellative semiring satisfying the equivalent conditions of 4.2(v) will be called *conical.*

4.3. PROPOSITION. *Let S be a non-trivial ac-semiring.*

(i) *If $0 \notin S$ and S is conical, then S is multiplicatively cancellative and $P(S)$ (see 4.1) is also conical.*

(ii) *If S is a parasemifield, then S is conical if and only if for every $a \in S$, $a \neq 1$, there exist $x, y \in S$ such that $a + x = 1 + ax + y$.*

(iii) *If S is congruence-simple then either S is conical or S is a zero-multiplication ring of prime order.*

Proof. The proof of both (i) and (ii) is easy. To prove (iii), let I be an ideal of the ring $R = R(S)$ (see 4.2) and define a relation r on S by $(x, y) \in r$ if and only if $x - y \in I$. Then r is a congruence of S, $I = 0$ if $r = \mathrm{id}_S$, and $I = R$ if $r = S \times S$. Thus R is ideal simple and the rest is clear. ∎

4.4. LEMMA. *Let S be a non-trivial ac-semiring such that $0 \notin S$, and let $w \in R = R(S)$ be such that $w^2 \in S$. Put $S_1 = \{a + bw;\ a, b \in S \cup \{0\}, a + b \neq 0\}$ and $S_2 = \{a - bw;\ a, b \in S \cup \{0\}, a + b \neq 0\}$. Then*:

(i) *Both S_1 and S_2 are subsemirings of R and $S \subseteq S_1 \cap S_2$.*

(ii) *If $0 \in S_1 \cap S_2$, then $cw = 0$ for at least one $c \in S$.*

(iii) *If S is an mc-semiring, then either $0 \notin S_1$ or $0 \notin S_2$.*

Proof. If $a_1 + b_1 w = 0 = a_2 - b_2 w$ for some $a_1, a_2, b_1, b_2 \in S$ then $-b_1 b_2 w^2 \in S$ and $b_1 b_2 w^2 \in S$, a contradiction with $0 \notin S$. Furthermore, if $w = e - f$, $e, f \in S$, and $cw = 0$, $c \in S$, then $e \neq f$ (since $w \neq 0$) and $ce = cf$. ∎

In the remaining part of this section, let S be a non-trivial amc-semiring. Then $S(+)$ contains no neutral element (since otherwise $S0 = 0$) and the relation $\leq_S$ defined on S by $x \leq_S y$ if and only if $y = x + z$ for some $z \in S \cup \{0\}$ is an ordering; this ordering is compatible with respect to both the addition and the multiplication of S. Moreover, $\leq_S$ can be extended to an ordering (denote it also by $\leq_S$) of the difference ring $R = R(S)$ (see 4.2); we have $x \leq_S y$ in R if and only if $y - x \in S \cup \{0\}$. The following lemma is obvious:

4.5. LEMMA. (i) *S is upward-cofinal in $R(\leq_S)$.*

(ii) *The following conditions are equivalent*:

(ii1) *$\leq_S$ is linear on R.*

(ii2) *$\leq_S$ is linear on S.*

(ii3) *For every $u \in R$, $u \neq 0$, either $u \in S$ or $-u \in S$.*

(ii4) *S is semisubtractive. (That is, for all $a, b \in S$, $a \neq b$, there exists $x \in S$ such that either $a + x = b$ or $b + x = a$.)*

4.6. LEMMA. *Let S be an ac-parasemifield. If $a, b \in S$ are such that $b^2 \leq_S a^2$, then $b \leq_S a$.*

Proof. We have $a^2 = b^2 + z$ for some $z \in S \cup \{0\}$, and then $a(a + b) = a^2 + ab = b^2 + z + ab = b(a + b) + z = (b + z(a + b)^{-1})(a + b)$. Consequently, $a = b + z(a + b)^{-1}$, $z(a + b)^{-1} \in S \cup \{0\}$, and $b \leq_S a$. ∎

4.7. LEMMA. *Let S be an ac-parasemifield. Then $2 \cdot 1_S \leq_S a + a^{-1} + (n \cdot 1_S)^{-1}$ for every $a \in S$ and every positive integer n.*

Proof. For positive integers m, n put $f(m) = 2^m$ and $b_n = (2n - 1)1_S \cdot (n \cdot 1_S)^{-1} \in S$. Now, if $n \geq 1$, then (using standard methods) we can find $m \geq 1$ such that

$$((2n - 1)/n)^{f(m)} \leq \binom{f(m)}{f(m - 1)}.$$

On the other hand, using the binomial formula for $(a + a^{-1})^{f(m)}$, we also find that

$$\binom{f(m)}{f(m-1)} \cdot 1_S \leq_S (a + a^{-1})^{f(m)}.$$

Consequently, $b_n^{f(m)} \leq_S (a + a^{-1})^{f(m)}$ and, by 4.6, we have $b_n \leq_S a + a^{-1}$. ∎

The semiring S is said to be *archimedean* if for all $a, b \in S$ there exists a positive integer n such that $b \leq_S na$ (equivalently, for all $a, b \in S$, there exist $c \in S$ and a positive integer m such that $b + c = ma$). Note that if this is true, then for all $x \in R$ and $a \in S$ there exists $n \geq 1$ with $x \leq_S na$.

4.8. LEMMA. *Let S be an archimedean conical ac-parasemifield. Then*

(i) $2 \cdot 1_S \leq_S a + a^{-1}$ *for every* $a \in S$.

(ii) $2ab \leq_S a^2 + b^2$ *for all* $a, b \in S$.

Proof. By 4.2(v), there exists a field F such that S is a subsemiring of F and $F = \{a - b;\ a, b \in S\}$. Clearly, the characteristic of F is zero and hence we can assume that $\mathbb{Q}$ (the field of rationals) is the prime subfield of F.

Let n be a positive integer and $a \in S$, $a \neq 1$. By 4.7, $a + a^{-1} = (2n - 1)/n + c_n$ for some $c_n \in S$. Put $v = a + a^{-1} - 2 \in F$, $v \neq 0$, since $a \neq 1$. Then $v + 1/n = c_n$, $nv + 1 = nc_n \in S$. Further, $-v^{-1} \in F$ and $-v^{-1} = d - e$, $d, e \in S$, $e = d + v^{-1}$. Since S is archimedean, we have $d \leq_S m$ for a suitable positive integer m, $m = d + f$, $f \in S$. Now, $v^{-1} + m = v^{-1} + d + f = e + f \in S$, $1 + vm = v(e + f)$. As we have already proved, $1 + vm \in S$, and so $v = (1 + vm)(e + f)^{-1} \in S$. Thus $a + a^{-1} = v + 2$ and $2 \leq_S a + a^{-1}$.

Finally, let $a, b \in S$, $a \neq b$, $w = a - b \in F$. Then $w^2a^{-1}b^{-1} + ba^{-1} - 2 \in S$ by the preceding part of the proof. ∎

5. CONGRUENCE-SIMPLE MULTIPLICATIVELY CANCELLATIVE ADDITIVELY IDEMPOTENT COMMUTATIVE SEMIRINGS

5.1. EXAMPLE. Let A be a non-zero subsemigroup of the additive group $\mathbb{R}(+)$ of real numbers. We shall consider the following (commutative) mcai-semiring $W = W(A) = W(\oplus, *)$: $W = A$, $a \oplus b = \min(a, b)$, and $a * b = a + b$ for all $a, b \in A$.

5.1.1. LEMMA. *W is congruence-simple if and only if $A \cap \mathbb{R}^+ \neq \emptyset \neq A \cap \mathbb{R}^-$.*

Proof. First, assume that W is congruence-simple. If $A \cap \mathbb{R}^- = \emptyset$, $0 \neq a \in A$, and if a relation r is defined on W by $(x, y) \in r$ if and only if either $x = y$ or $2a \leq \min(x, y)$, then r is a non-trivial congruence of W, a contradiction. We proceed similarly if $A \cap \mathbb{R}^+ = \emptyset$.

Now, assume that $A \cap \mathbb{R}^+ \neq \emptyset \neq A \cap \mathbb{R}^-$ and let $r \neq \mathrm{id}_W$ be a congruence of W. Take $a, b \in W$; $a < b$; and $c \in A \cap \mathbb{R}^+$. Since $r \neq \mathrm{id}_W$ and $A \cap \mathbb{R}^- \neq \emptyset$, there are $e, f \in W$ such that $(e, f) \in r$, $e < f \leq a$, and $c + b - a \leq f - e$. Let n be the greatest non-negative integer such that $e + nc \leq a$. Then $(n + 1)c + e + b - a \leq f + nc$, $0 < (n + 1)c + e - a \leq f + nc - b$, $b < f + nc$. Of course, $(e + nc, f + nc) \in r$, $(e + nc) \oplus a = e + nc$, $(f + nc) \oplus a = a$, $(e + nc, a) \in r$. Quite similarly, $(e + nc, b) \in r$ and $(a, b) \in r$. Thus $r = W \times W$. ∎

5.1.2. LEMMA. (i) *W is ideal-simple if and only if A is a subgroup of $\mathbb{R}(+)$ (i.e., W is a parasemifield).*

(ii) *W is finitely generated if and only if so is the semigroup $A(+)$.*

5.1.3. LEMMA. (i) *$W(\oplus)$ possesses a neutral element if and only if $A \cap \mathbb{R}^+ = \emptyset$ and $\sup(A) \in A$.*

(ii) *$W(\oplus)$ possesses an absorbing element if and only if $A \cap \mathbb{R}^- = \emptyset$ and $\inf(A) \in A$.*

(iii) *$W(*)$ possesses a neutral element if and only if $0 \in A$.*

(iv) *$W(*)$ does not possess an absorbing element.*

5.1.4. LEMMA. *If A and B are subsemigroups of $\mathbb{R}(+)$ such that $A \cap \mathbb{R}^+ \neq \emptyset \neq B \cap \mathbb{R}^+$ and $A \cap \mathbb{R}^- \neq \emptyset \neq B \cap \mathbb{R}^-$, then $W(A) \cong W(B)$ if and only if $B = qA$ for some $q \in \mathbb{R}^+$.*

5.2. PROPOSITION. *Let S be a cg-simple ai-parasemifield. Then the semilattice $S(+)$ is a chain, i.e., $a + b \in \{a, b\}$ for all $a, b \in S$.*

Proof. The relation $\leq$ defined on S by $x \leq y$ if and only if $x + y = x$ is an ordering (compatible with addition and multiplication) and we have to show that this ordering is linear. Anyway, note first that since $S(\cdot)$ is a group, $S(+)$ contains no smallest (i.e., absorbing) element and also no greatest (i.e., neutral) element. Now, take $w \in S$ and put $T = \{a \in S; aw \leq w\}$. Then $1 \in T$ and T is a subsemiring of S. Moreover, $Tx \cap Ty = T(x + y)$ for all $x, y \in S$.

Indeed, if $a, b \in T$ and $ax = by = v$, then $v(x + y)^{-1}w \leq wx(x + y)^{-1}$, $v(x + y)^{-1}w \leq wy(x + y)^{-1}$, $v(x + y)^{-1}w \leq w(x + y)(x + y)^{-1} = w$, $v = v(x + y)^{-1}(x + y) \in T(x + y)$. Conversely, if $c \in T$, then $c(x + y)x^{-1}w = cw + cyx^{-1}w \leq w$, $c(x + y) \in Tx$, and, similarly, $c(x + y) \in Ty$.

Now, defining a relation r on S by $(x, y) \in r$ if and only if $Tx = Ty$, we get a congruence of the semiring S. If $r = S \times S$, then $T = S$, $aw \leq w$ for

every $a \in S$, and w is a greatest element of S, a contradiction. Thus $r = \mathrm{id}_S$ and $x \mapsto Tx$ is an injective mapping.

Let $x, y \in S$. If $x \leq y$ and $a \in S$, then $y^{-1} \leq x^{-1}$, $axy^{-1}w \leq axx^{-1}w = aw \leq w$, $axy^{-1} \in T$, and we see that $Tx \subseteq Ty$. Conversely, if $Tx \subseteq Ty$, then $Tx = Tx \cap Ty = T(x + y)$, and hence $x = x + y$, $x \leq y$. Then $x \leq y$ if and only if $Tx \subseteq Ty$ and our aim is to show that the set $\{Tx; x \in S\}$ is linearly ordered by inclusion. As one may see easily, this is true if and only if $T \cup T^{-1} = S$ and now, proceeding by contradiction, we shall assume that $a \in S \setminus (T \cup T^{-1})$.

For every $n \geq 0$, let $P_n = T \cap Ta \cap \cdots \cap Ta^n = T(1 + a + \cdots + a^n)$ and, for $x \in S$, let Q_x denote the set of $u \in S$ such that $P_m \subseteq Txu$ for at least on $m \geq 0$. Then s_a is a congruence of S, where $(x, y) \in s_a$ if and only if $Q_x = Q_y$, and we shall first assume that $s_a = \mathrm{id}_S$.

Clearly, $Q_{1+a} \subseteq Q_1$. Conversely, if $P_m \subseteq Tu$, then $P_{m+1} \subseteq P_m a \subseteq Tau$, $P_{m+1} \subseteq P_m \subseteq Tu$, $P_{m+1} \subseteq Tau \cap Tu = T(1 + a)u$, and $u \in Q_{1+a}$. Thus, $(1 + a, 1) \in s_a$ and consequently $1 + a = 1$. However, then $T = T(1 + a) = T \cap Ta \subseteq Ta$ and $a \in T^{-1}$, a contradiction.

We have proved that $s_a = S \times S$, and therefore $(x, 1) \in s_a$ for every $x \in S$ and there exists $m \geq 0$ such that $P_m \subseteq Tx$. Proceeding similarly (i.e., replacing a by a^{-1}), we can show that $R_n \subseteq Tx$ for some $n \geq 0$, $R_n = T \cap Ta^{-1} \cap \cdots \cap Ta^{-n} = T(1 + a^{-1} + \cdots + a^{-n})$. In particular, $P_k \subseteq Ta^{-1}$ for some $k \geq 0$ and we have $P_k a \subseteq T \cap P_k a = P_{k+1} \subseteq P_k$, $P_k \subseteq P_k a^{-1}$, and, by induction, $P_k \subseteq P_k a^{-i} \subseteq Ta^{-i}$ for every $i \geq 0$. Consequently, $P_k \subseteq Tx$, i.e., $Tb \subseteq Tx$, $b = 1 + a + \cdots + a^k$, for every $x \in S$. In this way, we have shown that b is a smallest element of S and this is the needed final contradiction. ∎

5.3. THEOREM. *Let S be a congruence-simple multiplicatively cancellative additively idempotent semiring* (*see* 3.3). *The there exists a subsemigroup A of the additive group $\mathbb{R}(+)$ of real numbers such that $A \cap \mathbb{R}^+ \neq \emptyset \neq A \cap \mathbb{R}^-$ and the semirings S and $W(A)$ are isomorphic* (*see Example* 5.1).

Proof. First, assume that S is a parasemifield. By Proposition 5.2, the semilattice $S(+)$ is a chain (possessing no smallest and no greatest element), and so $S(\cdot)$ is a linearly ordered (abelian) group ($x \leq y$ if and only if $x + y = x$). We are going to make it clear that this order is archimedean.

Let $w \in S$, $1 < w$. Define a relation t_w on S by $(x, y) \in t$ if and only if either $x = y$ or $vw^m \leq x \leq vw^n$ and $vw^m \leq y \leq vw^n$ for an element $v \in S$ and some positive integers m, n, $m \leq n$. Then t_w is a congruence of S and we have $t_w = S \times S$. In particular, given $x \in S$, we have $vw^m \leq x \leq vw^n$, $vw^m \leq w \leq vw^n$, $v \leq w^{1-m}$ and $x \leq w^{1+n-m}$.

We have proved that $S(\cdot, \leq)$ is an archimedean linearly ordered (abelian) group. According to the well-known Hölder (−Baer−Cartan−Loonstra)

Theorem ([19; see also [2, 4, 24]), there exists an injective homomorphism φ of $S(\cdot)$ into the additive group $\mathbb{R}(+)$ such that $x \leq y$ in $S(\leq)$ implies $\varphi(x) \leq \varphi(y)$ in $\mathbb{R}(\leq)$. (If, among the positive elements of $S(\cdot, \leq)$, there exists a smallest one, say w, then $S(\cdot)$ is an infinite cyclic group generated by w and we put $\varphi(w^n) = n$. In the opposite case, we choose any $w > 1$ and, for every $x \in S$, we put $\varphi(x) = \sup\{m/n;\ m, n \in \mathbb{Z},\ n > 0, w^m \leq x^n\}$. Consequently, $S \cong W(\varphi(S(\cdot)))$.

The general case now follows from an easy combination of Proposition 4.1, the preceding part of the proof, and Example 5.1. ∎

6. A FEW CONSEQUENCES

6.1. COROLLARY (cf. [26, 3.2]). *Let S be a congruence-simple semiring such that the additive semigroup $S(+)$ possesses a neutral element. Then just one of the following three cases takes place*:

(1) *S is isomorphic to one of the two-element semirings Z_3, Z_4, Z_5, and Z_6*;

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

(3) *S is a field*.

Proof. Combine 3.1, 3.3, 5.3, 5.1.3, and 3.4. ∎

6.2. COROLLARY (cf. [26, 4.7]). *Let S be a congruence-simple semiring such that the multiplicative semigroup $S(\cdot)$ possesses an absorbing element. Then just one of the following two cases takes place*:

(1) *S is isomorphic to one of the two-element semirings Z_1, Z_2, Z_3, Z_4, and Z_5.*

(2) *There exists an abelian group G such that S is isomorphic to the semiring $V(G)$ (see* 3.2).

Proof. Combine 3.1, 3.3, 5.3, and 5.1.3. ∎

6.3. COROLLARY. *Let S be a congruence-simple semiring such that the multiplicative semigroup $S(\cdot)$ possesses an absorbing element. Then just one of the following four cases takes place*:

(1) *S is isomorphic to one of the two-element semirings Z_1, Z_2, Z_3, Z_4, and Z_5.*

(2) *There exists an abelian group G such that S is isomorphic to the semiring $V(G)$ (see* 3.2).

(3) *S is a zero-multiplication ring of finite prime order*.

(4) *S is a field*.

Proof. Combine 3.1, 3.3, 5.3, 5.1.3, and 3.4. ∎

6.4. *Remark.* Let S be a congruence-simple semiring such that $S(+)$ contains a neutral (resp. absorbing) element 0 (resp. o). Then $S0 = 0$ (resp. $So = o$) in all cases with the exception of the two-element semirings Z_3, Z_6 (resp. Z_4, Z_5).

7. SEMIRINGS OF POSITIVE REAL NUMBERS

The results of this section are of auxiliary character and to some extent are folklore. Anyway, for the benefit of the reader, full details are given.

7.1 Let F be a field containing as a (prime) subfield the field $\mathbb{Q}$ of rationals and let $\mathfrak{A}$ denote the set of subsemirings S of F such that $0 \notin S$; we have $\mathbb{Q}^+ \in \mathfrak{A}$ and $\mathfrak{A}$ is ordered by inclusion. Further, let $\mathfrak{L}$ (resp. $\mathfrak{C}$) denote the set of $S \in \mathfrak{A}$ such that $1 \in S$ (resp. $\mathbb{Q}^+ \subseteq S$), and for every $a \in S$, let there be a positive integer n (resp., positive integers $p, q \in \mathbb{Q}^+$) such that $a \leq_S n$ (resp., $p \leq_S a \leq_S q$). Finally, let $\mathfrak{M}$ denote the set of $S \in \mathfrak{A}$ such that $F = \{a - b;\ a, b \in S\}$.

7.1.1. LEMMA. (i) *Every $S \in \mathfrak{C}$ is archimedean.*

(ii) *If $S \in \mathfrak{L}$ and $S(\cdot)$ is a group, then S is archimedean and $S \in \mathfrak{C}$.*

(iii) *Every $S \in \mathfrak{M}$ is conical.*

Proof. (i) If $a, b \in S$, then $p \leq_S a$ and $b \leq_S q$ for some $p, q \in \mathbb{Q}^+$ and we get $b \leq_S qp^{-1}a$.

(ii) If $a, b \in S$, then $ba^{-1} \leq_S n$ and $b \leq_S na$.

(iii) This is obvious. ∎

7.1.2. LEMMA. *Let $S \in \mathfrak{M}$ and $T \in \mathfrak{A}$ be such that $S \subseteq T$. Then:*

(i) $T \in \mathfrak{M}$.

(ii) *If $S \in \mathfrak{L}$, then $T \in \mathfrak{L}$.*

(iii) *If $S \in \mathfrak{L}$ and $\mathbb{Q}^+ \subseteq S$, then $T \in \mathfrak{C}$ (in particular, $S \in \mathfrak{C}$).*

Proof. (i) This is obvious.

(ii) If $u \in T$, then $u = a - b$; $a, b \in S$; $a \leq_S n$; and $u = a - b \leq_T n$.

(iii) Let $w \in F$; $w \neq 0$; $w^{-1} = a - b$; $a, b \in S$; $a <_S n$; $n = a + c$, $c \in S$. Now, for $d = b + c \in S$, we have $w^{-1} + d = n$; $n^{-1}w^{-1} + n^{-1}d = 1$; $n^{-1} + n^{-1}dw = w$; $n^{-1}d \in S$; and hence $n^{-1} \leq_T w$, provided that $w \in T$. ∎

7.1.3. LEMMA. *Let $S \in \mathfrak{U}$ and $T = \{pa + q;\ p, q \in \mathbb{Q}^+ \cup \{0\},\ p + q \neq 0,\ a \in S\}$. Then T is a subsemiring of F; $S \cup \mathbb{Q}^+ \subseteq T$; and $T \in \mathfrak{A}$. Moreover, if $S \in \mathfrak{L}$ (resp., $\mathfrak{C}$, $\mathfrak{M}$), then $T \in \mathfrak{L}$ (resp., $\mathfrak{C}$, $\mathfrak{M}$).*

Proof. If $pa + q = 0$ for $p + q \neq 0$, then $p \neq 0 \neq q$ and there is a positive integer n such that $-n \in S$. Now, $(-n)^2 = n^2 \in S$ and $n.(-n) = -n^2 \in S$, a contradiction. The rest is clear. ∎

7.1.4. LEMMA. *Let* $S \in \mathfrak{A}$, $w \in F$, $w^2 \in S$, *and* $T = \{a + bw;\ a, b \in S \cup \{0\},\ a + b \neq 0\}$. *Then*:

(i) *T is a subsemiring of F and* $S \subseteq T$ (*if* $1 \in S$, *then* $w \in T$).

(ii) *If* $0 \in T$, *then* $-w = ab^{-1}$ *for some* $a, b \in S$.

(iii) *If* $S(\cdot)$ *is a group and* $-w \notin S$, *then* $T \in \mathfrak{A}$.

7.1.5. LEMMA. *Let* $S \in \mathfrak{A}$; $w \in F$; $w^2 \in S$; $T_1 = \{a + bw;\ a, b \in S \cup \{0\},\ a + b \neq 0\}$; *and* $T_2 = \{a - bw;\ a, b \in S \cup \{0\},\ a + b \neq 0\}$. *Then both* T_1 *and* T_2 *are subsemirings of* F, $S \subseteq T_1 \cap T_2$ *and either* $T_1 \in \mathfrak{A}$ *or* $T_2 \in \mathfrak{A}$.

Proof. See the proof of Lemma 4.4. ∎

7.1.6. LEMMA. *Let* $S \in \mathfrak{A}$ *be such that* $1 \in S$, *and let* $u \in S$. *Denote by T the set of all elements from F of the form* $a_0 + a_1u^{-1} + \cdots + a_nu^{-n}$, *where* $n \geq 0$, $a_i \in S \cup \{0\}$, *and* $a = \sum a_i \neq 0$ (*then* $a \in S$). *Then T is a subsemiring of F*, $S \cup \{u^{-1}\} \subseteq T$, *and* $T \in \mathfrak{A}$. *Moreover, if* $S \in \mathfrak{C}$, *then* $T \in \mathfrak{C}$.

Proof. If $a_0 + a_1u^{-1} + \cdots + a_nu^{-n} = 0$, then $a_0u^n + a_1u^{n-1} + \cdots + a_{n-1}u + a_n = 0$, a contradiction with $0 \notin S$. Thus $T \in \mathfrak{A}$ and, moreover, if $p \leq_S u \leq_S q$ then $q^{-1} \leq_T \leq u^{-1} \leq_T p^{-1}$, and the rest is clear. ∎

7.1.7. LEMMA. *Let* $S \in \mathfrak{A}$ *and* $T = \{ab^{-1};\ a, b \in S\}$. *Then* $T \in \mathfrak{A}$ *and* $T(\cdot)$ *is a group* (*i.e., T is a parasemifield*). *Moreover, if S is archimedean, then T is archimedean and* $T \in \mathfrak{C}$.

Proof. The proof is easy. ∎

7.1.8. PROPOSITION. *Let* $S \in \mathfrak{L} \cap \mathfrak{M}$ *be maximal in* $\mathfrak{L} \cap \mathfrak{M}$. *Then*:

(i) $S(\cdot)$ *is a group and S is an archimedean conical parasemifield.*

(ii) *For every* $w \in F$, $w \neq 0$, *we have* $w^2 \in S$ *and either* $w \in F$ *or* $-w \in F$.

(iii) $\leq_S$ *is linear* (*both on S and F*).

Proof. By Lemma 7.1.3, $\mathbb{Q}^+ \subseteq S$ and, by 7.1.2(iii), $S \in \mathfrak{C}$. Further, by 7.1.6., $S(\cdot)$ is a group and by 7.1.1, S is both archimedean and conical. Now, $w^2 \in S$ by 4.8(ii) and we shall consider the semirings T_1, T_2 defined in 7.1.5. We can assume that $0 \notin T_1 = \{a + bw;\ a, b \in S \cup \{0\},\ a + b \neq 0\}$, the other case being similar. Then $T \in \mathfrak{M}$, $S \subseteq T$, and $w \in T$. Finally, by 7.1.2(iii), $T \in \mathfrak{C} \cap \mathfrak{M}$ and, due to the maximality of S, we must have $T = S$ and $w \in S$. ∎

7.2. Let F be a field and let S be a subsemiring of F such that $S \in \mathfrak{L} \cap \mathfrak{M}$; then $\text{char}(F) = 0$ and we may assume that $\mathbb{Q}$ is a subfield of

F. Now, let $T \in \mathfrak{L} \cap \mathfrak{M}$ be such that $S \subseteq T$ and T is maximal in $\mathfrak{L} \cap \mathfrak{M}$. By 7.1.8 the ordering $\leq_T$ corresponding to T is an archimedean linear order on the field F. Now, by the Hölder Theorem ([19]; see the proof of 5.3) there exists an injective homomorphism $\varphi\colon F(+) \mapsto \mathbb{R}(+)$ such that $\varphi(x) \leq \varphi(y)$ in the usual order of $\mathbb{R}$ whenever $x, y \in F$ and $x \leq_T y$. Further (see [1] and [4]), for every $a \in F$ there is $\alpha(a) \in \mathbb{R}$ such that $\varphi(ax) = \varphi(x)\alpha(a)$ for every $x \in F$; we have $\alpha(0) = 0$, $\alpha(a) > 0$ for $a >_T 0$, and $\alpha(a + b) = \alpha(a) + \alpha(b)$ for all $a, b \in F$. Consequently, we can find $q \in \mathbb{R}$, $q > 0$, such that $\alpha(a) = \varphi(a)q$ for every $a \in F$. Thus $\varphi(xy) = \varphi(x)\varphi(y)q$ for all $x, y \in F$, and the mapping $\psi\colon F \to \mathbb{R}$, $\psi(x) = \varphi(x)q$ for every $x \in F$ is an (injective) homomorphism of the field F into the field $\mathbb{R}$; for $x \leq_T y$ in F we have $\psi(x) \leq \psi(y)$ in $\mathbb{R}$. In particular, $\psi(S) \subseteq \psi(T) \subseteq \mathbb{R}^+$.

7.3 Let F be a subfield of the field $\mathbb{R}$ of real numbers and let $P(F) = \{a_1^2 + \cdots + a_n^2;\ n \geq 1,\ a_i \in F,\ a_i \neq 0\}$.

7.3.1. LEMMA. (i) *$P(F)$ is a conical parasemifield.*

(ii) $F = \{a - b;\ a, b \in P(F)\}$.

(iii) $\mathbb{Q}^+ \subseteq P(F) \subseteq F^+$.

Proof. If $a = a_1^2 + \cdots + a_n^2$, then $a^{-1} = (a_1 a^{-1})^2 + \cdots + (a_n a^{-1})^2 \in P(F)$. Further, $x = (x/2)^2 + 1 - (x/2 - 1)^2$ for every $x \in F$. ∎

7.3.2. LEMMA. *$F^+ = \{a \in F;\ a > 0\}$ is an archimedean and conical parasemifield.*

7.3.3. LEMMA. *Let S be a subsemiring of F such that $P(F) \subseteq S \subseteq F^+$. Then S is a conical parasemifield.*

Proof. We have $a^{-1} = a.a^{-2} \in S$ for every $a \in S$. ∎

7.3.4. LEMMA. *Let S, T be subsemirings of F such that $P(F) \subseteq S \subseteq F^+$ and $P(F) \subseteq T \subseteq F^+$. Then*:

(i) *S and T are conical.*

(ii) *If $S \subseteq T$ and S is archimedean, then T is also.*

(iii) *If S, T are archimedean, then $S \cap T$ is also.*

7.3.5. LEMMA. *Let S be a subsemiring of F such that $0 \notin S$ and $1 \in S$. Denote by $A(S)$ the set of $a \in S$ such that $n - a \in S$ for some positive integer n. Then $A(S)$ is a subsemiring of S, $1 \in A(S)$, and there is a positive integer m with $m - a \in A(S)$.*

7.3.6. EXAMPLE. Let $F = \mathbb{Q}$ and $S = \{q \in F;\ q \geq 1\}$. Then S is a subsemiring of F, S is both archimedean and conical, and $S + S \neq S$.

7.3.7. EXAMPLE. Let $F = \mathbb{Q}(\sqrt{2})$. Then $P(F) \neq F^+ (-1 + \sqrt{2} \in F^+ \setminus P(F))$ and $P(F)$ is an archimedean and conical parasemifield ($(a + b\sqrt{2})^2 + (a - b\sqrt{2})^2 = 2a^2 + 4b^2$ and Lemma 7.3.5 applies).

7.3.8. EXAMPLE. Let $\alpha \in \mathbb{R}^+$ be a transcendental number and $F = \mathbb{Q}(\alpha)$. Then $P(F)$ is a conical parasemifield but $P(F)$ is not archimedean (we have $n - \alpha^{-2} \notin P(F)$ for every positive integer n; to show this, just watch the behavior of $f^2(r)g^{-2}(r)$, where $f, g \in \mathbb{Q}[x]$, $f \neq 0 \neq g$, and $r \in \mathbb{R}$, $r \to 0$). Further, for every $a \in P(F)$, choose a positive integer m_a such that $m_a - a \in F^+$ and let S be the subsemiring of F^+ generated by $P(F) \cup \{m_a - a;\ a \in P(F)\}$. Then S is both archimedean and conical.

7.3.9. EXAMPLE. If $F = \mathbb{Q}$, $\mathbb{R}$ or if F is the field of algebraic real numbers, then $P(F) = F^+$.

7.3.10. EXAMPLE. Let $\alpha \in \mathbb{R}^+$ be a transcendental number, $0 < \alpha < 1$, $F = \mathbb{Q}(\alpha)$, and let $\varphi\colon \mathbb{Q}(x) \to F$ be the isomorphism such that $\varphi(x) = \alpha$ and $\varphi|\mathbb{Q} = \mathrm{id}$. Now, denote by T the set of $f \in \mathbb{Q}(x)$ such that there exist $m, n \in \mathbb{N}$ with $n^{-1} \leq f(u) \leq m$ for every $u \in \mathbb{R}$, $0 \leq u \leq 1$. Then $S = \varphi(T)$ is a subsemiring of F^+ and S is an archimedean parasemifield. On the other hand, S is not conical and $P(F) \not\subseteq S$.

7.4. LEMMA. *Let S, T be subsemirings of $\mathbb{R}$ such that $S \subseteq T$, S is conical, and every element of T is algebraic over the difference field $F = S - S$ $(= R(S))$. Then T is conical.*

Proof. Put $R = T - T$ and take $0 \neq r \in R$. Then $r = a - b$, $a, b \in T$, and there is a polynomial $f \in F[x, y]$ such that $r^{-1} = f(a, b)$. Since $F = S - S$, we conclude easily that $r^{-1} \in R$. Thus R is a field and T is conical. ∎

7.5. LEMMA. *Let S and T be subsemirings of $\mathbb{R}^+$ such that both S and T are semisubtractive (see 4.5), $\mathbb{Q}^+ \subseteq S \cap T$, and there exists a (semiring) isomorphism $\varphi\colon S \to T$. Then $S = T$ and $\varphi = \mathrm{id}$.*

Proof. Assume, on the contrary, that $\varphi(a) < a$ for some $a \in S$. Now, take $q \in \mathbb{Q}^+$ such that $\varphi(a) < q < a$. Then $a - q \in S$ and $0 < \varphi(a - q) = \varphi(a) - q < 0$, a contradiction. ∎

7.6. *Remark.* Let F be a field such that $0 \notin P(F) = \{a_1^2 + \cdots + a_n^2;$ $n \geq 1,\ 0 \neq a_i \in F\}$ ($P(F)$ is a conical parasemifield and $F = P(F) - P(F)$), and let $\mathfrak{A}$ denote the set of subsemirings S of F such that $P(F) \subseteq S$ and $0 \notin S$. Again, every $S \in \mathfrak{A}$ is a conical parasemifield and S is maximal in $\mathfrak{A}$ if and only if $S \in \mathfrak{M}$, where $\mathfrak{M}$ is the set of semisubtractive parasemifields from $\mathfrak{A}$.

Take $S \in \mathfrak{A}$ and $w \in F$ such that $w \notin S$ and $-w \notin S$. Then $S_1 = \{a - bw;\ a, b \in S \cup \{0\},\ a + b \neq 0\} \in \mathfrak{A}$; $S \subseteq S_1$; $-w \in S_1$; and $S_1 \subseteq T$, where T is maximal in $\mathfrak{A}$; we have $T \in \mathfrak{M}$ and $w \notin T$. Now, it follows easily that $S = \bigcap \mathfrak{M}_S$, where $\mathfrak{M}_S = \{T \in \mathfrak{M};\ S \subseteq T\}$.

8. CONGRUENCE-SIMPLE MULTIPLICATIVELY AND ADDITIVELY CANCELLATIVE COMMUTATIVE SEMIRINGS

8.1. LEMMA. *Let S be a cg-simple amc-semiring. Then S is archimedean.*

Proof. Define a relation r on S by $(a, b) \in r$ if and only if there exist $c, d \in S$ and $m, n \in \mathbb{N}$ such that $a + c = mb$ and $b + d = na$. It is easy to check that r is a congruence of S such that $(a, 2a) \in r$ for every $a \in S$. Since $a \neq 2a$, we have $r = S \times S$. ∎

8.2. THEOREM. *Let S be a non-trivial amc-semiring. Then S is congruence-simple if and only if S satisfies the following three conditions*:

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

(2) *For all $a, b, c, d \in S$, $a \neq b$, there exist $e, f \in S$ such that $ae + bf + c = af + be + d$ (i.e., S is conical).*

(3) *For all $a, b \in S$ there exist $c, d \in S$ such that $bc + d = a$ (i.e., S is bi-ideal-simple).*

Proof. If S is cg-simple, then (1) is satisfied by 8.1, (2) by 4.3(iii), and 4.2(v), and (3) follows from the easy fact that $Sb + S$ is a bi-ideal of S. Now, conversely, assume that the conditions (1), (2), and (3) are satisfied. The rest of the proof is divided into four parts:

(i) Let $r \neq \mathrm{id}_S$ be a congruence of S such that the corresponding factor-semiring $T = S/r$ is additively cancellative. The difference ring $R = R(S)$ of S is a field (by (ii) and 4.2(v)) and the set $I = \{a - b;\ (a, b) \in r\}$ is a non-zero ideal of R. Consequently, $I = R$ and for all $x, y \in S$ there are $a, b \in S$ such that $(a, b) \in r$ and $x - y = a - b$. Now, $x + b = y + a$ and $(x, y) \in r$, since T is an ac-semiring. We have proved that $r = S \times S$.

(ii) Let T be a non-trivial semiring satisfying the conditions (1), (3) (and (2)) and let $w \in T$ be such that $w + w = w$. We claim that T is a ring (field).

First, according to (1), for every $x \in T$ there exists $y \in T$ such that $x + y = w$. In particular, if $x + x = x$, then $w + x = x + y + x = x + y = w$. On the other hand, replacing w by x, we get $x + w = x$. Thus $x = w$ is

the only idempotent of the additive semigroup $T(+)$ and it follows easily that $Tw = w$ and, by (3), $w + T = T$. Consequently, $w = 0$ is a neutral element of $T(+)$ and we conclude that $T(+)$ is an (abelian) group and T is a ring. Finally, if T satisfies (2), $a \in T$, $a \neq 0$, and $c \in T$, then $ae + c = ae + 0f + c = af + 0e + 0 = af$ and $c = a(e - f)$ for some $e, f \in T$. Thus T is a field.

(iii) Let r be a congruence of S such that $(w, 2w) \in r$ for at least one $w \in S$. We claim that $r = S \times S$.

Assume on the contrary, that $r \neq S \times S$ and put $T = S/r$. By (ii), T is a ring, and hence $r = \mathrm{id}_S$ by (i), a contradiction, since S is not a ring.

(iv) Let s be a congruence of S, $s \neq S \times S$, and let $w \in S$ be arbitrary. By (iii), $(w, 2w) \notin s$ and we can consider a congruence r of S maximal with respect to $s \subseteq r$ and $(w, 2w) \notin r$. Now, again by (iii), r is a maximal congruence of S and $T = S/r$ is a cg-simple semiring such that $T(+)$ has no idempotent. Using 3.1 we see that T is an ac-semiring, and so $r = s = \mathrm{id}_S$ by (i). Thus S is cg-simple. ▮

8.3. COROLLARY. *Let S be an ac-parasemifield. Then S is cg-simple if and only if the following two conditions are satisfied*:

(1) *For every $a \in S$ there exist $b \in S$ and a positive integer n such that $a + b = n1_S$ (i.e., S is archimedean).*

(2) *For every $a \in S$, $a \neq 1_S$, there exist $b, c \in S$ such that $a + b = 1_S + ab + c$ (i.e., S is conical).*

8.4. *Remark*. Let S be a non-trivial amc-semiring such that $1_S \in S$. Then S is cg-simple if and only if S is both archimedean and conical and, moreover, $S + S = S$ (i.e., $1_S = a + b$ for some $a, b \in S$).

To show this, we can proceed similarly as in the proof of 8.2. Note that $(1_S, 2_S) \notin r$ for every congruence $r \neq S \times S$ and, if r is maximal with respect to $(1_S, 2_S) \notin r$, then r is a maximal congruence of S.

8.5. THEOREM. *Let S be a congruence-simple additively and multiplicatively cancellative semiring and let $F = R(S)$ (see 4.2). Then F is a field and there exists an (injective) homomorphism φ of the field F into the field $\mathbb{R}$ of real numbers such that $\varphi(S) \subseteq \mathbb{R}^+$. Moreover, if S is a parasemifield, then $P(F) = \{a_1^2 + \cdots + a_n^2;\ 0 \neq a_i \in F,\ n \geq 1\} \subseteq S$.*

Proof. In view of 4.1, we may assume that S is a parasemifield. By Proposition 4.3, S is conical, and hence F is a field. Further, by Lemma 8.1, S is archimedean and the rest is clear from 4.8 and 7.2. ▮

8.6. THEOREM [21, 6.9; 10, Satz 16]. *Let E be a subfield of $\mathbb{R}$ and S be a subsemiring of $\mathbb{R}$ such that S is a parasemifield, $E^+ \subseteq S$, and every element*

from S is algebraic over E. Then S is congruence-simple (*i.e., S is archimedean and conical*).

8.7. COROLLARY [23, Satz 2]. *Let S be a subsemiring of* $\mathbb{R}$ *such that S is a parasemifield and every element from S is algebraic over* $\mathbb{Q}$. *Then S is congruence-simple*.

8.8. COROLLARY (cf. 7.3.8). *Let F be a subfield of* $\mathbb{R}$ *such that F is algebraic over* $\mathbb{Q}$. *Then* $P(F) = \{a_1^2 + \cdots + a_n^2;\ 0 \neq a_i \in F\}$ *is a congruence-simple parasemifield* (*in particular*, $P(F)$ *is achimedean*).

8.9. *Remark*. Let E, F be subfields of $\mathbb{R}$ such that $E \subseteq F$ and the linear dimension $\dim(F_E)$ is finite. Denote by $\mathfrak{M}$ the set of subsemirings S of F such that $F = S - S$, S is a parasemifield, and $E^+ \subseteq S$.

(i) We have $F = E(w)$ for some $w \in F^+$ and we denote by $(w =)$ $w_1, w_2, \ldots, w_n$, $n \geq 1$, all (pair-wise different) real roots of the minimal polynomial of w over E. Now, there exist exactly n different homomorphisms $\varphi_1, \ldots, \varphi_n$: $F \to \mathbb{R}$ such that $\varphi|E = \mathrm{id}$ and we may assume that $\varphi_1 = \mathrm{id}$ and $\varphi_i(w) = w_i$. Let $T_i = \varphi_i^{-1}(\mathbb{R}^+) = \varphi_i^{-1}(E(w_i)^+)$. Clearly, T_i are semisubtractive parasemifields, $T_1 = F^+$, $T_i \in \mathfrak{M}$, T_i are maximal in $\mathfrak{M}$, and $P(F) \subseteq T_i$.

(ii) Let T_M designate the intersection $\bigcap_{i \in M} T_i$ for every non-empty subset M of $N = \{1, 2, \ldots, n\}$. By [10, Satz 16], $T_{M_1} \neq T_{M_2}$ for $M_1 \neq M_2$ and $\mathfrak{M} = \{T_M;\ \emptyset \neq M \subseteq N\}$. Consequently, $\mathfrak{M}$ contains just $2^n - 1$ elements and $T_N = T_1 \cap \cdots \cap T_n$ is a smallest element of $\mathfrak{M}$. Clearly, $P(F) \subseteq T_N = \{a_1^2 b_1 + \cdots + a_m^2 b_m;\ m \geq 1,\ 0 \neq a_i \in F,\ b_i \in E^+\}$. Note also that if S is a subsemiring of F such that $T_N \subseteq S$ and $0 \notin S$, then S is a parasemifield and $S \in \mathfrak{M}$, so that $S = T_M$ for some $\emptyset \neq M \subseteq N$. Similarly, if S is a subsemiring of F such that $T_N \subseteq S$ and $0 \in S$, then either $S = T_M \cup \{0\}$ or $S = F$.

(iii) If $E^+ \subseteq P(F)$ (e.g., $E = \mathbb{Q}$), then $T_N = P(F)$ and $\mathfrak{M}$ is the set of subsemirings S of F such that $F = S - S$ $(= R(S))$ and S is a parasemifield.

(iv) (cf. 7.5). Let M_1 and M_2 be non-empty parts of N such that there exists an isomorphism φ: $T_{M_1} \colon \to T_{M_2}$ of the parasemifields with $\varphi|E^+ = \mathrm{id}$. Then φ extends to an E-automorphism of F, and therefore there is $k \in N$ such that $w_k \in F$ and $\varphi = \varphi_k|T_{M_1}$. Further, there is a permutation p of N such that $\varphi_i \varphi_k^{-1} = \varphi_{p(i)}$ and $\varphi_k(T_i) T_{p(i)}$ for every $i \in N$. Now, if $M_1 = \{i_1, i_2, \ldots, i_m\}$, then $M_2 = \{p(i_1), p(i_2), \ldots, p(i_m)\}$; in particular, the sets M_1 and M_2 have the same number of elements.

8.10. *Remark*. Let E, F be subfields of $\mathbb{R}$ such that $E \subseteq F$ and F be algebraic over E. Denote by $\mathfrak{M}$ the set of subsemirings of F such that

$F = S - S$, S is a parasemifield, and $E^+ \subseteq S$, and denote by Φ the set of homomorphisms $\varphi\colon F \to \mathbb{R}$ such that $\varphi|E = \mathrm{id}$. Let $T_\varphi = \varphi^{-1}(\mathbb{R}^+)$ for every $\varphi \in \Phi$. Clearly, T_φ are subsemisubtractive parasemifields, $T_{\mathrm{id}} = F^+$, $T_\varphi \in \mathfrak{M}$, T_φ are maximal in $\mathfrak{M}$, and $P(F) \subseteq T_\varphi$.

Let T_M designate the intersection $\bigcap_{\varphi \in M} T_\varphi$ for every non-empty subset M of Φ. Clearly, $T_M \in \mathfrak{M}$ and $P(F) \subseteq T_M$. Now, we show that $\mathfrak{M} = \{T_M; \varnothing \neq M \subseteq \Phi\}$.

Let $S \in \mathfrak{M}$, $a, b \in S$, and $F_1 = E(a^{-1}b)$, $S_1 = S \cap F_1$. Then $E^+ \subseteq S_1$ and S_1 is archimedean by [10, Satz 16]. In particular, $n - a^{-1}b \in S_1$ and $na - b \in S$ for some $n \in \mathbb{N}$. We have shown that S is archimedean, and therefore $P(F) \subseteq S$ (4.8(ii)). Now, it follows from 4.5 that $S = T_M$ for some $\varnothing \neq M \subseteq \Phi$.

8.11. THEOREM (cf. 9.7). *Let S be an archimedean and conical amc-semiring such that S has a unit element 1_S and $(n1_S)^{-1} \in S$ for every $n \in \mathbb{N}$. Then S is a parasemifield.*

Proof. We make use of a variation on the well-known Goodearl–Handelman method (see [13] for details and further references), the backgrounds of which go back to Hölder and Hilbert ([19] and [18]; but see also [1–9, 15, 22, 24, 29–31]).

Since S is conical, there exists a field F such that S is a subsemiring of $F = S - S$ (see 4.2(i, v)) and, since S is archimedean, we have $S \subseteq A$, where A denotes the set of $a \in F$ such that for every $x \in F$ there is $n \in \mathbb{N}$ with $na - x \in S$. Now, an (additive) homomorphism $f\colon F(+) \to \mathbb{R}(+)$ will be called normative if $f(1_F) = 1$ and $f(a) > 0$ for every $a \in S$. The set $\mathscr{N}$ of normative homomorphisms is a compact convex set and we denote by $\mathscr{E}$ the set of extremal points of $\mathscr{N}$. Now, one can show that every $f \in \mathscr{E}$ is a ring homomorphism; see e.g. [14] (in fact, no topological arguments are necessary and a rather easy and purely algebraic proof of the mentioned fact is available—the kind reader may wish to make it up as a stimulating exercise).

The rest of the present proof is divided into two parts:

(i) First, we check that $a \in A$ if and only if $f(a) > 0$ for every normative ring homomorphism $f\colon F \to \mathbb{R}$.

Indeed, if $a \in A$, then $na - 1_F \in S$ for some $n \in \mathbb{N}$ and we have $f(a) \geq n^{-1} > 0$. To show the converse implication, put $r = \sup\{n/m; n \in \mathbb{Z}, m \in \mathbb{N}, ma - n1_F \in S \cup \{0\}\}$. Then there exists $f \in \mathscr{E}$ such that $f(a) = r$, and therefore $f > 0$ and $ma - n1_F \in S \cup \{0\}$ for some $m, n \in \mathbb{N}$. Now, it follows easily that $a \in A$.

(ii) Now, according to (i), $A(\cdot)$ is a subgroup of $F(\cdot)$, and A is a parasemifield, and it remains to show that $A = S$. But, if $a \in A$, then $na \in S$ for some $n \in \mathbb{N}$ and consequently $a = n^{-1} \cdot na \in S$. ∎

8.12. COROLLARY. *Let S be a congruence-simple amc-semiring such that $1_S \in S$. Then S is a parasemifield if and only if $(n1_S)^{-1} \in S$ for every $n \in \mathbb{N}$.*

8.13. COROLLARY. *Let S be a congruence-simple amc-semiring such that $1_S \in S$. Then for every $a \in S$ there exist $b \in S$ and $n \in \mathbb{N}$ such that $ab = n1_S$.*

8.14. EXAMPLE. Let $\alpha \in \mathbb{R}^+$ be a transcendental number and $F = \mathbb{Q}(\alpha)$. There exists an isomorphism $\varphi: \mathbb{Q}(x) \to F$ such that $\varphi(x) = \alpha$ and $\varphi \mid \mathbb{Q} = \mathrm{id}$. Now, we denote by S the set of $a \in F$ such that $a \in \mathbb{R}^+$ and $\varphi(a) \in \mathbb{R}^+$, where $\varphi(a) = \varphi((\varphi^{-1}(a))')$ (here, for $f \in \mathbb{Q}(x)$, f' is the derivative of f). Clearly, S is a subsemiring of F^+, S is both archimedean and conical, and $\mathbb{Q}^+S \subseteq S$. Moreover, given $a, b \in S$, we find $q \in \mathbb{Q}^+$ small enough such that $qa^2 < b$ and $q\partial(a^2) < \partial(b)$. That is, $b - (qa)a \in S$ and we see that S is bi-ideal-simple. But 8.2, S is a congruence-simple amc-semiring. Finally, note that $S \cap \mathbb{Q} = \varnothing$; in particular, S is not a parasemifield.

9. SUBSEMIRINGS OF $\mathbb{Q}^+$

9.1. LEMMA. *A subsemiring S of $\mathbb{Q}^+$ is archimedean and conical if and only if for every $n \in \mathbb{N}$ there exists $m \in \mathbb{N}$ such that $k/n \in S$ for every $k \geq m$.*

Proof. Assume first that S is both archimedean and conical. For $n \in \mathbb{N}$, we can find $r, s \in S \cap \mathbb{N}$ such that $(rn - 1)/n \in S$ and $((rn - 1)s - 1)/(rn - 1) \in S$. Now, put $a = n((rn - 1)s - 1)$ and $b = (rn - 1)^2$. Then $\gcd(a, b) = 1$, and hence there is $m \in \mathbb{N}$ such that $\{m, m + 1, m + 2, \ldots\} \subseteq \{ua + vb;\ u, v \in \mathbb{N}\}$. Since $a/n(rn - 1) \in S$ and $b/n(rn - 1) \in S$, we have $k/n(rn - 1) \in S$ for every $k \in m$. Consequently, $k/n \in S$.

Now, assume that the condition of the lemma is satisfied and let $a, b, r, s \in \mathbb{N}$, $a/b \in S$. Then there is m such that $k/bs \in S$ for every $k \geq m$. Taking $l \in \mathbb{N}$ such that $las - br \geq m$, we get $l \cdot a/b - r/s \in S$. ∎

9.2. PROPOSITION. *Let S be a subsemiring of $\mathbb{Q}^+$ such that S is archimedean and conical and $1/r \in S$ for some $r \in \mathbb{N}$, $r \geq 2$. Then $S = \mathbb{Q}^+$.*

Proof. If $n \in \mathbb{N}$, then $r^l/n \in S$ for some $l \in \mathbb{N}$ (by 9.1), and therefore $1/n = (1/r^l)(r^l/n) \in S$. ∎

9.3. LEMMA. *Let $a, b, c \in \mathbb{N}$ be such that $a < b$, $c < b$ and $\gcd(a, c) = 1$. Then $1/b \in S$, where S denotes the subsemiring of $\mathbb{Q}^+$ generated by a/b and c/b.*

Proof. Let $n \in \mathbb{N}$ be such that $n \geq 2$ and $\binom{n}{2} \geq (n + 1)(b - 1)^4$. We will construct a sequence $r_0, \ldots, r_n$ of integers such that $0 \leq r_i \leq c$ for

every $0 \le i \le n$. First, since $\gcd(a^{n+1}, c) = 1$, there is $0 \le r_0 < c$ such that $b^n \equiv r_0 a^{n+1} (\mathrm{mod}\, c)$. Quite similarly, $\gcd(a^n, c) = 1$, $(b^n - r_0 a^{n+1})/c \equiv r_1 a^n \pmod{c}$ for some $0 \le r_1 < c$, and $b^n \equiv (r_0 a^{n+1} + r_1 a^n c) \pmod{c^2}$. Proceeding by induction, we find the remaining numbers $r_2, \ldots, r_n$ such that

$$b^n \equiv \left(r_0 a^{n+1} + r_1 a^n c + \cdots + r_i a^{n+1-i} c^i\right) \left(\mathrm{mod}\, c^{i+1}\right)$$

for every $0 \le i \le n$. Now, put $s = \sum_{i=0}^{n} r_i a^{n+1-i} c^i$. Since $a < b$ and $c < b$, we have $s \le \sum_{i=0}^{n} (b-1)(b-1)^{n+1-i}(b-1)^i = (n+1)(b-1)^{n+2} \le \binom{n}{2}(b-1)^{n-2} \le (b-1+1)^n = b^n$, and therefore $t = b^n - s \ge 0$. On the other hand, $t = r_{n+1} c^{n+1}$ and $b^n = s + r_{n+1} c^{n+1}$. Finally, it is clear from the definition of s that $(s + r_{n+1} c^{n+1})/b^{n+1} \in S$ and we have proved that $1/b \in S$. ∎

9.4. LEMMA. *Let $a, b, c, d \in \mathbb{N}$ be such that $a < b$, $c < d$ and $\gcd(a, b) = \gcd(c, d) = \gcd(a, c) = 1$. Then $1/\mathrm{scm}(b, d) \in S$, where S denotes the subsemiring of $\mathbb{Q}^+$ generated by a/b and c/d.*

Proof. We have $a/b = e/g$, $c/d = f/g$, and $\gcd(e, f) = 1$, where $g = \mathrm{scm}(b, d)$. It remains to use 9.3. ∎

9.5. THEOREM. *Let S be a congruence-simple subsemiring of $\mathbb{Q}^+$ such that $1 \in S$. Then $S = \mathbb{Q}^+$.*

Proof. By 8.2, S is both archimedean and conical and there exist $a, b, c, d \in \mathbb{N}$ such that $a/b \in S$, $c/d \in S$, $a/b + c/d = 1$, and $\gcd(a, b) = 1 = \gcd(c, d)$. It remains to apply Lemma 9.4 and Proposition 9.2. ∎

9.6. EXAMPLE. Every positive rational number q can (uniquely) be written as $q = 2^{d(q)} \cdot rs^{-1}$, where $d(q) \in \mathbb{Z}$, $r, s \in \mathbb{N}$, and $\gcd(r, s) = \gcd(r, 2) = \gcd(s, 2) = 1$. Clearly, $d(p + q) \ge \min(d(p), d(q))$, $d(pq) = d(p) + d(q)$ for all $p, q \in \mathbb{Q}^+$, and we put $|q|_2 = 2^{-d(q)}$ (the dyadic norm). Now, the set $S = \{q \in \mathbb{Q}^+;\ q - |q|_2 > 0\}$ is a (proper) subsemiring of $\mathbb{Q}^+$ (e.g., $2, 3, 4, \cdots \in S$, $2/3 \in S$, $1 \notin S$, $1/2 \notin S$) and, for every $t \in \mathbb{Q}$, one finds easily $n \in \mathbb{N}$ such that $n - t \in S$. Thus S is both archimedean and conical. Furthermore, if $p, q \in S$ and $w = p - |p|_2$, then $w \in \mathbb{Q}^+$ and we take $t \in S$ such that $tq \le w$ and $d(p) \le d(tq)$. Now, $p - tq \in S$ and we see that S is bi-ideal simple. By Theorem 8.2, S is a congruence-simple amc-semiring ($\mathbb{Q}^+ \notin S$ and S is not a parasemifield).

9.7. *Remark.* Using Proposition 9.2, we can improve Theorem 8.11 as follows:

Let S be an archimedean and conical amc-semiring such that $(n1_S)^{-1} \in S$ for at least one $n \in \mathbb{N}$, $n \ge 2$. We claim that S is a parasemifield.

Indeed, with respect to 7.2 (see also the proof of 8.11) we may assume that S is a subsemiring of $\mathbb{R}^+$. Now, $F = S - S$ is a subfield of $\mathbb{R}$ and we

put $S_1 = S \cap \mathbb{Q}^+$. Then $1 \in S_1$, $1/n \in S_1$, and S_1 is an archimedean and conical subsemiring of $\mathbb{Q}^+$. By Proposition 9.2, $S_1 = \mathbb{Q}^+$, and S is a parasemifield.

10. CONGRUENCE-SIMPLE COMMUTATIVE SEMIRINGS—SUMMARY

10.1. THEOREM. *A (commutative) semiring S is congruence-simple if and only if S is (isomorphic to) one of the following semirings*:

(1) *the two-element semirings Z_1, Z_2, Z_3, Z_4, and Z_5 (see Section 2).*

(2) *the semirings $V(G)$ for any abelian group G (see 3.2);*

(3) *the semirings $W(A)$ for any subsemigroup A of the additive group $\mathbb{R}(+)$ of real numbers such that $A \cap \mathbb{R}^+ \neq \emptyset \neq A \cap \mathbb{R}^-$ (see Example 5.1);*

(4) *fields*;

(5) *zero-multiplication rings of finite prime order*;

(6) *the subsemirings S of the semiring $\mathbb{R}^+$ of positive real numbers such that the following three conditions are satisfied*:

(6a) *for all $a, b \in S$ there exist $c \in S$ and a positive integer n such that $b + c = na$;*

(6b) *for all $a, b, c, d \in S$, $a \neq b$, there exist $e, f \in S$ such that $ae + bf + c = af + be + d$;*

(6c) *for all $a, b \in S$ there exist $c, d \in S$ such that $bc + d = a$.*

Proof. Combine 3.1, 3.2, 3.4, 5.3, 8.3, and 8.6. ∎

10.2. *Remark*. (i) The two-element semirings $Z_1, \ldots, Z_5$ are pair-wise non-isomorphic.

(ii) $V(G_1) \cong V(G_2)$ if and only if $G_1 \cong G_2$ (see 3.2).

(iii) $W(A_1) \cong W(A_2)$ if and only if $A_2 = qA_1$ for some $q \in \mathbb{R}^+$ (see 5.1.4).

10.3. *Remark*. The congruence-simple semirings of type 10.1(6) are not yet fully classified up to isomorphism (see 8.9 and 8.10 for some special cases). In particular, the following problem (originally formulated in [26, 5.7]) remains open: Does there exist a congruence-simple amc-semiring S such that $1_S \in S$ and S is not a parasemifield? According to 9.5 and 9.7 we know that if S were such a semiring, then $S \not\subseteq \mathbb{Q}^+$ and $(n1_S)^{-1} \notin S$ for every $n \in \mathbb{N}$, $n \geq 2$. Examples of cg-simple amc-semirings without unit are given in 8.14 and 9.6.

11. IDEAL-SIMPLE COMMUTATIVE SEMIRINGS—BASIC CLASSIFICATION

Ideal-simple semirings are better known than the congruence-simple ones—see e.g. [10–12, 16, 17, 20, 21, 23, 27, 28, 32, 34–41]. Anyway, for the sake of completeness and the full comfort of the reader, we include some basic information on ideal-simple (commutative) semirings. The reader is urged to compare the results on the congruence-simple semirings with those on the ideal-simple ones.

A non-trivial (commutative) semiring S is said to be a *semifield* if there exists an element $w \in S$ such that $Sw = w$ and T is a subgroup of $S(\cdot)$, where $T = S \setminus \{w\}$. If, moreover, S is not a field, then one says that S is a *proper semifield*.

11.1. PROPOSITION. (i) *Every semifield is ideal-simple.*

(ii) *Every parasemifield is ideal-simple.*

11.2. THEOREM. *Let S be an ideal-simple semiring. Then just one of the following five cases takes place*:

(1) *S is isomorphic to one of the two-element semirings Z_1, Z_3, and Z_4;*

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

(3) *S is a field*;

(4) *S is a proper semifield*;

(5) *S is a parasemifield.*

Proof. Suppose that S contains at least three elements and put $A = \{a \in S;\ |Sa| = 1\}$. If $b \in S \setminus A$, then $Sb = S$, and hence S is a parasemifield, provided that $A = \emptyset$. Assume therefore that $A \neq \emptyset$; then there is an element $w \in S$ such that $SA = \{w\}$, $w = w + w$, and we see that A is an ideal of S. Consequently, either $A = \{w\}$ or $A = S$.

First, let $A = S$ and $S + w = w$ (i.e., $w = o$ is an absorbing element of $S(+)$). Then $SS = o$ and, if P is a subsemigroup of $S(+)$ such that $o \in S$, then P is an ideal of S, and hence either $P = \{o\}$ or $P = S$. If $a \in S$, $a + a = a$, then $\{a, o\}$ is a subsemigroup of $S(+)$, $\{a, o\} \neq S$, and therefore $a = o$. We have proved that w is the only idempotent element of $S(+)$. Now, take $a \in S$, $a \neq o$, and put $P = \{na;\ n \geq 1\}$. Then $P \cup \{o\} = S$, $P(+)$ contains no proper subsemigroup, $P(+)$ is a finite cyclic semigroup, $o \in P$, and there is $b \in P$ such that $b \neq o$ and $b + b = o$. But then $\{b, o\}$ is a subsemigroup of $S(+)$, a contradiction with $|S| \geq 3$.

Next, let $A = S$ and $S + w \neq w$. Then $S + w = S$, since $S + w$ is a (bi-) ideal of S, and it follows that $w = 0$ is a neutral element of $S(+)$. Further, proceeding similarly as in the preceding part of the proof, we can show

that 0 is only the only idempotent of $S(+)$ and that every cyclic subsemigroup of $S(+)$ is finite. Consequently, $S(+)$ is a group and S is a ring. Thus either (2) or (3) takes place.

Further, let $A = \{w\}$ and $S + w = w$, $w = o$. For every $a \in T = S\setminus\{o\}$, the set $I_a = \{b \in S;\ ab = o\}$ is an ideal of S, $I_a \neq S$, and so $I_a = o$. We have checked that T is a subsemigroup of $S(\cdot)$ and, since $Ta = T$ for every $a \in T$, $T(\cdot)$ is a group.

Finally, let $A = \{w\}$ and $S + w \neq w$. Then $S + w = S$, $w = 0$ is a neutral element of $S(+)$, and, proceeding similarly as in the preceding part, we show that $T = S\setminus\{0\}$ is a subgroup of $S(\cdot)$. ∎

12. SEMIFIELDS

12.1. PROPOSITION. *Let S be a semifield and let $w \in S$ be such that $Sw = w$ (and $T = S\setminus\{w\}$ is a subgroup of $S(\cdot)$). Then just one of the following four cases takes place*:

(1) *S is isomorphic to the two-element semiring Z_2 (and then $w = o$ is an absorbing element of both $S(+)$ and $S(\cdot)$)*;

(2) *$w = o$ is an absorbing element of both $S(+)$ and $S(\cdot)$, and $S + a \neq o$ for every $a \in T$*;

(3) *S is a field (and then $w = 0$ is a neutral element of $S(+)$)*;

(4) *$w = 0$ is a neutral element of $S(+)$ and S is a proper semifield (i.e., $S(+)$ is not a group)*.

Proof. We have $w + w = (1_S + 1_S)w = w$ and, if $1_S + w = w$, then $w = aw = a(1_S + w) = a + w$ for every $a \in S$, and so $w = o$. On the other hand, if $1_S + w \neq w$, then $1_S = (1_S + w)^{-1}(1 + w) = 1_S + w^{-1} + w$, $1_S + w = 1_S + w^{-1} + w + w = 1_S + w^{-1} + w = 1_S$, and $a + w = a1_S + aw = a(1_S + w) = a1_S = a$ for every $a \in S$, and so $a = 0$. The rest is clear. ∎

12.2. PROPOSITION. *Let S be a semifield of type* 12.1(2). *Define a relation ρ_S on S by $(a, b) \in \rho_S$ if and only if $\{x \in S;\ a + x = o\} = \{y \in S;\ b + y = o\}$. Then*

(i) *ρ_S is a congruence of S and $(a, o) \notin \rho_S$ for every $a \in T = S\setminus\{o\}$.*

(ii) *$P = \{a \in T;\ (a, 1_S) \in \rho_S\}$ is a subgroup of $T(\cdot)$ and either $P = 1$ (and $\rho_S = \mathrm{id}_S$) or P is a parasemifield.*

(iii) *The factor-semiring $R = S/\rho_S$ is isomorphic to the (additively idempotent) semifield $V(T/P)$ (see* 3.2) *and $\rho_R = \mathrm{id}_R$.*

Proof. The assertions (i), (ii) and the fact that $\rho_R = \mathrm{id}_R$ are easy to check. Further, let r be a congruence of the semiring R, $r \neq \mathrm{id}_R$. We have

$(x, y) \in r$ for some $x, y \in R$, $x \neq y$, and we put $A = \{r \in R; (z, o) \in R\}$. Then A is an ideal of R and, since $(x, y) \notin \rho_R = \mathrm{id}_R$, we have $A \neq \{o\}$. Thus $A = R$ (since R is ideal-simple) and $r = R \times R$. We have proved that R is a cg-simple semiring and the result follows from 3.1, 3.2, and 3.3. ∎

12.3. *Remark*. Let P be a semiring such that either P is trivial or P is a parasemifield. Suppose further that $P(\cdot)$ is a subgroup of an (abelian) group $T(\cdot)$, put $S = T \cup \{o\}$, and define an addition on S as follows:

(a) $x + o = o = o + x$ for every $x \in S$;

(b) $x + y = o$ for all $x, y \in T$, $x^{-1}y \notin P$;

(c) $x + y = (1_T + x^{-1}y)x = (1_T + y^{-1}x)y$ for all $x, y \in T$, $x^{-1}y \in P$.

Then S becomes a semifield of type 12.1(2) and every semifield of that type may be constructed in the described way.

12.4. PROPOSITION. *Let S be a proper semifield of type* 12.1(4). *Then*:

(i) $a + b \neq 0$ *for all* $a, b \in T = S \setminus \{0\}$.

(ii) *T is a subsemiring of S and either T is trivial* (*and then* $S \cong Z_5$) *or T is a parasemifield.*

Proof. Since $S(+)$ is not a group, the set $T_1 = \{a \in T; 0 \notin S + a\}$ is non-empty. Now, $bT_1 = T_1$ for every $b \in T$, and so $T_1 = T$. The rest is clear. ∎

12.5. *Remark*. Let T be a semiring such that either T is trivial or T is a parasemifield. Then $S = T \cup \{0\}$ is a semifield of type 12.1(4) and every semifield of this type may be constructed in the described way.

13. PARASEMIFIELDS

13.1. PROPOSITION [41]. *There exists a one-to-one correspondence between additively idempotent parasemifields and lattice-ordered non-trivial abelian groups*.

Proof. If S is an ai-parasemifield, then $S(\cdot, \wedge, \vee)$ is a lattice-ordered group, where $a \wedge b = a + b$ and $a \vee b = (a^{-1} + b^{-1})^{-1}$ for all $a, b \in S$. Conversely, if $S(\cdot, \wedge, \vee)$ is a lattice-ordered group and $a + b = a \wedge b$, then $S(+, \cdot)$ is an ai-parasemifield. ∎

13.2. *Remark*. Let S be an additively cancellative parasemifield and let Q^+ denote the sub-parasemifield of S generated by 1_S.

(i) $Q^+ \cong \mathbb{Q}^+$ (the parasemifield of positive rationals).

(ii) $Q = Q^+ \cup Q^- \cup \{0\}$ is a subfield of the ring $R = R(S)$ (see 4.2) and $Q \cong \mathbb{Q}$, so that R is an algebra over the field of rationals.

(iii) S is imbeddable into a field if and only if R is a domain and this is further equivalent to the condition that $ab + 1_S \neq a + b$ for all $a, b \in S \setminus \{1_S\}$.

13.3. EXAMPLE. Put $S = \mathbb{Q}^+ \times \mathbb{Q}^+$. Then S is an ac-parasemifield, and S is archimedean but S is not imbeddable into a field (in particular, S is not conical).

13.4. EXAMPLE. Let S be the set of fractions of the form f/g, where $f, g \in \mathbb{Q}^+[x]$. Then S is a subsemiring of $\mathbb{Q}(x)$ (and hence S is imbeddable into a field), S is an ac-parasemifield but S is not conical (e.g., $1/x - 1 \notin R(S) \subseteq \mathbb{Q}(x)$).

13.5. PROPOSITION. *Let S be a parasemifield. Define a relation η_S on S by $(a, b) \in \eta_S$ if and only if there exist a non-negative integer m and elements $u, v \in S \cup \{0\}$ such that $2^m a = b + u$ and $2^m b = a + v$. Then*

(i) *η_S is a congruence of S.*

(ii) *S/η_S is either trivial (and then S is additively cancellative) or an ai-parasemifield (see* 13.1).

(iii) *If a, b, c belong to a block of η_S and $b \neq c$, then $a + b \neq a + c$.*

(iv) *$P = \{a \in S; (a, 1_S) \in \eta_S\}$ is a subsemiring of S, $P(\cdot)$ is a subgroup of $S(\cdot)$, and either P is trivial (and then S is additively idempotent) or P is an ac-parasemifield (see* 13.2).

Proof. (Iii) Let $a + b = a + c$. We have $a + u = 2^m b$, $b + 2^m b = b + a + u = c + a + u = c + 2^m b$, $2(b + 2^{m-1}b) = b + b + 2^m b = b + c + 2^m b = c + c + 2^m b = 2(c + 2^{m-1}b)$, $b + 2^{m-1}b = c + 2^{m-1}b, \ldots, 2b = b + c$. Quite similarly, $2c = b + c$, and hence $b = c$. The rest is clear. ∎

14. FINITE AND FINITELY GENERATED SIMPLE SEMIRINGS

14.1. THEOREM. *The following conditions are equivalent for a semiring S:*

(i) *S is finite and congruence-simple.*

(ii) *S is finite and ideal-simple.*

(iii) *S is (isomorphic to) one of the following semirings:*

(iii1) *the two-element semirings Z_1, Z_2, Z_3, Z_4, and Z_5;*

(iii2) *finite fields;*

(iii3) *zero-multiplication rings of finite prime order;*

(iii4) *the semirings (semifields) $V(G)$ (see* 3.2*), G being a finite abelian group*.

Proof. Combine 3.1, 3.2, 3.3, 3.4, 5.3, and 11.2. ∎

14.2. THEOREM. *The following conditions are equivalent for a semiring S*:

(i) *S is finitely generated, congruence-simple, and infinite*.

(ii) *S is (isomorphic to) one of the following semirings*:

(ii1) *the semirings (semifields) $V(G)$ (see* 3.2*), G being an infinite finitely generated abelian group*;

(ii2) *the semirings $W(A)$ (see* 5.1*), A being a finitely generated subsemigroup of $\mathbb{R}(+)$ such that $A \cap \mathbb{R}^+ \neq \emptyset \neq A \cap \mathbb{R}^-$*.

Proof. Combining 3.1, 3.2, 3.3, 3.4, 4.2, 4.3, 5.1, and 5.3, we can restrict ourselves to the case when S is a finitely generated subsemiring of a field F such that $F = \{a - b;\ a, b \in S\}$. Then, of course, F is finitely generated as a ring and consequently F is finite (this is a rather well-known result and the reader may try to prove it as an exercise). ∎

14.3. COROLLARY. *Let S be a congruence-simple semiring such that S is finitely generated but not additively idempotent. Then S is finite*.

14.4. *Remark* (cf. [25]). (i) Let S be a congruence-simple semiring such that $|S| > 2^{\aleph_0}$. Then either S is a field or $S \cong V(G)$ for an abelian group G ($|G| = |S|$). In both cases, S is ideal-simple.

(ii) $(\mathbb{Q}^+)^{\mathfrak{a}}$ is an (ideal-simple) parasemifield for any cardinal number $\mathfrak{a} \geq 1$.

14.5. PROPOSITION. *The following conditions are equivalent for a semiring S*:

(i) *S is finitely generated, ideal-simple, and additively cancellative*.

(ii) *S is either a finite-field or a finite zero multiplication ring of prime order*.

Proof. First, let S be an ac-parasemifield. We claim that S is not finitely generated as a semiring. Assume the contrary, put $R = R(S)$ and take a maximal ideal I of R. The relation r defined on S by $(a, b) \in r$ if and only if $a - b \in I$ is a congruence of S and $T = S/r$ is again an ac-parasemifield. On the other hand, $F = R(T) \cong R/I$ is a finitely generated ring and a field. Then F is finite, and $T(+)$ is a group, a contradiction with $0 \notin T$.

Now, let S be a finitely generated id-simple ac-semiring. Then S is not a parasemifield and, in view of 12.1 and 12.4, S is not a proper semifield

either. Thus, according to 11.2, S is a (finite) field or a zero multiplication ring of prime order. ∎

14.6. *Remark* (cf. 14.2, 14.3, 14.5). It seems to be an open problem whether every infinite finitely generated ideal-simple semiring is additively idempotent.

REFERENCES

1. B. Baer, Zur Topologie der Gruppen, *J. Reine Angew. Math.* **160** (1929), 208–226.
2. E. Becker, Partial orders on a field and valuation rings, *Comm. Algebra* **7** (1979), 1933–1976.
3. E. Becker and N. Schwartz, Zum Darstellungsatz von Kadison–Dubois, *Arch. Math.* **40** (1983), 421–428.
4. H. Cartan, Une théorème sur les groupes ordonnés, *Bull. Sci. Math.* **63** (1939), 201–205.
5. J. V. Chion, Arhimedovski uporjadočennye kol'ca, *Uspekhi Mat. Nauk* **9** (1954), 237–242.
6. D. W. Dubois, On partly ordered fields, *Proc. Amer. Math. Soc.* **7** (1956), 918–930.
7. D. W. Dubois, A note on David Harrison's theory of preprimes, *Pacific J. Math.* **21** (1967), 15–19.
8. D. W. Dubois, Second note on David Harrison's theory of preprimes, *Pacific J. Math.* **24** (1968), 57–68.
9. D. W. Dubois, Infinite primes and ordered fields, *Dissertationes Math.* (*Rozprawy Mat.*) **69** (1970).
10. R. Eilhauer, Zur Theorie der Halbkörper, I, *Acta Math. Acad. Sci. Hungar.* **19** (1968), 23–45.
11. K. Głazek, "A Short Guide through the Literature on Semirings," Math. Institute, University of Wroclaw, Poland, 1985.
12. J. Golan, "The Theory of Semirings with Applications in Math. and Theoretical Computer Science," Pitman Monographs and Surveys in Pure and Applied Math., Vol. 54, Longman, Harlow, 1992.
13. K. R. Goodearl, "Partially Ordered Abelian Groups with Interpolation," Mathematical Surveys and Monographs, Vol. 20, American Mathematical Society, Vol. 20, Providence, 1986.
14. D. Handelman, Positive polynomials and product type actions of compact groups, *Mem. Amer. Math. Soc.* **320** (1985).
15. D. K. Harrison, Finite and infinite primes for rings and fields, *Mem. Amer. Math. Soc.* **68** (1968).
16. U. Hebisch and H. J. Weinert, "Halbringe–Algebraische Theorie und Anwendungen in der Informatik," Teubner, Stuttgart, 1993.
17. U. Hebisch and H. J. Weinert, Semirings and semifields, *in* "Handbook of Algebra," Vol. 1, pp. 425–462, Elsevier, New York, 1996.
18. D. Hilbert, "Grundlagen der Geometrie," Teubner Verlag, Leipzig/Berlin, 1930.
19. O. Hölder, Die Axiome der Quantität und die Lehre vom Mass, *Ber. Verhandlungen König. Sächsischen Gesell. Wissen. Leipzig* **53** (1901), 1–64.
20. H. C. Hutchins, Division semirings with $1 + 1 = 1$, *Semigroup Forum* **22** (1981), 181–188.
21. H. C. Hutchins and H. J. Weinert, Homomorphisms and kernels of semifields, *Period. Math. Hungar.* **21** (1990), 113–152.
22. R. W. Kadison, A representation theory for commutative topological algebra, *Mem. Amer. Math. Soc.* **7** (1951).

23. H. Koch, Über Halbkörper, die in algebraischen Zahlkörpern enhalten sind, *Acta Math. Acad. Sci. Hungary.* **15** (1964), 439–444.
24. F. Loonstra, Ordered groups, *Proc. Nederl. Akad. Wetensch.* **49** (1945), 41–66.
25. R. McKenzie and S. Shelah, The cardinals of simple models for universal theories, *Proc. Tarski Sympos.* **25** (1974), 53–74.
26. S. S. Mitchell and P. B. Fenoglio, Congruence-free commutative semirings, *Semigroup Forum* **37** (1988), 79–91.
27. W. H. Reynolds, Embedding a partially ordered ring in a division algebra, *Trans. Amer. Math. Soc.* **158** (1988), 79–91.
28. W. H. Reynolds, A note on embedding a partial ordered ring in a division algebra, *Proc. Amer. Math. Soc.* **37** (1973), 37–41.
29. M. H. Stone, A general theory of spectra, I, *Proc. Nat. Acad. Sci. USA* **26** (1940), 28)–283.
30. M. H. Stone, A general theory of spectra, II, *Proc. Nat. Acad. Sci. USA* **27** (1941), 83–87.
31. G. Tallini, Sui sistemi a doppia composizione ordinati archimedei, *Atti Accad. Naz. Lincei Rend. Cl. Fis. Mat. Nat.* **18** (1955), 367–373.
32. T. Tamura, Notes on semirings whose multiplicative semirings are groups, *in* "Proceedings 5th Symposium on Semigroups, Sakado, Japan, 1981," pp. 56–66.
33. H. S. Vandiver, Note on a simple type of algebra in which the cancellation law of addition does not hold, *Bull. Amer. Math. Soc.* **40** (1934), 916–920.
34. H. J. Weinert, Über Halbringe und Halbkörper, I, *Acta Math. Acad. Sci. Hungar.* **13** (1962), 365–378.
35. H. J. Weinert, Über Halbringe und Halbkörper, II, *Acta Math. Acad. Sci. Hungar.* **14** (1963), 209–227.
36. H. J. Weinert, Über Halbringe und Halbkörper, III, *Acta Math. Acad. Sci. Hungar.* **15** (1964), 177–194.
37. H. J. Weinert, Ein Struktursatz für idempotente Halbkörper, *Acta Math. Acad. Sci. Hungar.* **15** (1964), 289–295.
38. H. J. Weinert, On 0-simple semirings, semigroup semirings, and two kinds of division semirings, *Semigroup Forum* **28** (1984), 313–333.
39. H. J. Weinert and R. Wiegandt, Complementary radical classes of proper semifields, *Colloq. Math. Soc. János Bolyai* **61** (1991), 297–310.
40. H. J. Weinert and R. Wiegandt, A. Kurosh-Amitsur radical theory for proper semifields, *Comm. Algebra* **20** (1992), 2419–2458.
41. H. J. Weinert and R. Wiegandt, On the structure of semifields and lattice-ordered groups, *Period. Math. Hungar.* **32** (1996), 147–162.