Notes on commutative parasemifields

Vítězslav Kala, Tomáš Kepka, Miroslav Korbelář

Abstract. Parasemifields (i.e., commutative semirings whose multiplicative semigroups are groups) are considered in more detail. We show that if a parasemifield S contains $\mathbb{Q}^+$ as a subparasemifield and is generated by $\mathbb{Q}^+ \cup \{a\}$, $a \in S$, as a semiring, then S is (as a semiring) not finitely generated.

Keywords: semiring, ideal-simple, parasemifield, finitely generated

Classification: 16Y60

The present short note is an immediate continuation of [1]. Henceforth, the reader is fully referred to [1] as concerns goal, motivation, notation, comments and further details. However, for better understanding, a few useful observations on parasemifields are collected here.

1. Introduction

A *semiring* is an algebraic structure with two associative operations (addition and multiplication), where the addition is commutative and the multiplication distributes over the addition from both sides. If the multiplication is commutative, the semiring is said to be commutative. Throughout this paper, all semirings are assumed to be commutative. Henceforth, the word 'semiring' will always mean a commutative one.

Throughout this paper, $\mathbb{Z}$ denotes the ring of integers, $\mathbb{N}$ ($\mathbb{N}_0$, resp.) denotes the semiring of positive (non-negative, resp.) integers. $\mathbb{Q}$ is the field of all rational numbers, $\mathbb{Q}^+$ ($\mathbb{Q}_0^+$, resp.) denotes the semiring of positive (non-negative, resp.) rationals.

Let S be a semiring. A non-empty subset I of S is an *ideal* if $(I+I) \cup SI \cup IS \subseteq I$.

Further, define a relation μ_S on S by $(a,b) \in \mu_S$ if and only if $b = a + z$ for some $z \in S \cup \{0\}$. Then μ_S is a stable quasiordering of the semiring S and $\nu_S = \ker \mu_S$ is a congruence of S. The following two lemmas are obvious.

This work is a part of the research project MSM00210839 financed by MŠMT, the first two authors were supported by the Grant Agency of Charles University #8648/2008 and the second one by the Grant Agency of Czech Republic #301-13/201718.

1.1 Lemma. *The following conditions are equivalent:*

(i) $\mu_S = S \times S$,

(ii) $\nu_S = S \times S$,

(iii) *S is a ring (i.e., $S(+)$ is an abelian group).*

1.2 Lemma. *μ_S is an ordering of S if and only if $\nu_S = \mathrm{id}_S$.*

1.3 Lemma. *Put $T = S/\nu_S$. Then*

(i) *$(a,b) \in \mu_S$ if and only if $(a/\nu_S, b/\nu_S) \in \mu_T$.*

(ii) *$\nu_T = \mathrm{id}_T$ and $\mu_T = \mu_S/\nu_S$.*

(iii) *μ_T is a stable ordering of the semiring T.*

Proof: Denote by π the natural projection of S onto T. If $(a,b) \in \mu_S$ then $b = a + z$, $z \in S \cup \{0\}$, $\pi(b) = \pi(a) + \pi(z)$ and $(\pi(a), \pi(b)) \in \mu_T$. Conversely, if $(\pi(a), \pi(b)) \in \mu_T$ then $\pi(a+z) = \pi(b)$ for some $z \in S \cup \{0\}$, and hence $(a+z, b) \in \nu_S$ and $a + z + v = b$, $v \in S \cup \{0\}$. Then, of course, $(a,b) \in \mu_S$. The rest is clear. □

Now, define a relation η_S on S by $(a,b) \in \eta_S$ if and only if there exist $m, n \in \mathbb{N}$ such that $(a, mb) \in \mu_S$ and $(b, na) \in \mu_S$.

1.4 Lemma. *$(a,b) \in \eta_S$ if and only if there exist $c, d \in S \cup \{0\}$ and $k \in \mathbb{N}_0$ such that $a + c = 2^k b$ and $b + d = 2^k a$.*

Proof: Easy to check. □

1.5 Lemma. (i) *η_S is a congruence of S, the factor-semiring S/η_S is additively idempotent and $\nu_S \subseteq \eta_S$.*

(ii) *η_S is the smallest congruence of S such that the corresponding factor is additively idempotent.*

Proof: (i) Easy to check.

(ii) Let r be a congruence of S such that S/r is additively idempotent. If $(a,b) \in \eta_S$ then $a + u = mb$, $b + v = na$ for some $u, v \in S \cup \{0\}$, $m, n \in \mathbb{N}$, and so $(a+u, b) \in r$ and $(b+v, a) \in r$. Moreover, $(a+u, a+b) \in r$ and $(b+v, b+a) \in r$. Thus $(na, mb) \in r$, which implies $(a,b) \in r$. □

1.6 Corollary. (i) *$\eta_S = \mathrm{id}_S$ if and only if S is additively idempotent.*

(ii) $\eta_S = \nu_S$ if and only if for every $a \in S$ there exists $z \in S \cup \{0\}$ such that $2a + z = a$.

(iii) The set $\{a \in S \mid 2a = a\}$ is either empty or an ideal of S.

1.7 Lemma. *Let $A(+)$ be a commutative semigroup such that the mapping $x \mapsto 2x$ is an injective transformation (in fact, an endomorphism) of A. If $b, c \in A$ and $m \in \mathbb{N}_0$ are such that $b + 2^m b = c + 2^m b$, then $b + b = c + b$.*

Proof: Assume that m is the smallest possible. If $m \geq 1$ then $2(b + 2^{m-1}b) = b + b + 2^m b = b + c + 2^m b = c + b + 2^m b = c + c + 2^m b = 2(c + 2^{m-1}b)$, and so $b + 2^{m-1}b = c + 2^{m-1}b$, a contradiction. Thus $m = 0$ and $b + b = c + b$. □

1.8 Lemma. *If A is a block of η_S then A is a subsemigroup of $S(+)$. If, moreover, the transformation $x \mapsto 2x$, $x \in A$, is injective, then $A(+)$ is a cancellative semigroup.*

Proof: Let $a + b = a + c$, $a, b, c \in A$. We have $(a, b) \in \eta_S$, and so there is $d \in S \cup \{0\}$ and $m \in \mathbb{N}_0$ such that $a + d = 2^m b$ (see 1.4). Then $b + 2^m b = b + a + d = c + a + d = c + 2^m b$. Hence $b + b = b + c$ by 1.7 and $c + c = c + b$ symmetrically. Thus $2b = 2c$ and $b = c$. □

1.9 Remark. We have $\eta_S = S \times S$ if and only if S is additively archimedean. When S is such and $x \mapsto 2x$, $x \in S$, is injective, then S is additively cancellative.

Define a relation ρ_S on S by $(a, b) \in \rho_S$ if and only if $a + z = b + z$ for some $z \in S \cup \{0\}$.

1.10 Lemma. (i) ρ_S is a congruence of S and the factor-semiring is additively cancellative.

(ii) ρ_S is the smallest congruence of S such that the factor-semiring is additively cancellative.

Proof: Easy to check. □

1.11 Corollary. *$\rho_S = \mathrm{id}_S$ if and only if S is additively cancellative.*

1.12 Lemma. (i) $\rho_S = S \times S$ if and only if $(a, 2a) \in \rho_S$ for all $a \in S$.

(ii) If S is additively idempotent, then $\rho_S = S \times S$.

Proof: (i) The direct implication is trivial. Conversely, if $(a, 2a) \in \rho_S$ for all $a \in S$, then $(a + b, 2a + b) \in \rho_S$, $a, b \in S$, and $(a + b, 2b + a) \in \rho_S$, symmetrically. Thus $(a + (a + b), b + (a + b)) \in \rho_S$, and so $(a, b) \in \rho_S$.

(ii) Clearly, $a + (a + b) = b + (a + b)$ for all $a, b \in S$. □

1.13 Lemma. *If $a + b = b$ for $a, b \in S$, then $(a, 2a) \in \rho_S$.*

Proof: We have $2a + b = a + b$, and hence $(a, 2a) \in \rho_S$. □

1.14 Lemma. *Assume that $1_S \in S$. Then the following conditions are equivalent:*

(i) *$\rho_S = S \times S$;*
(ii) *$(1_S, 2_S) \in \rho_S$;*
(iii) *$1_S + c = c$ for some $c \in S$;*
(iv) *for every $a \in S$ there exists $b \in S$ such that $a + b = b$;*
(v) *$(a, 2a) \in \rho_S$ for all $a \in S$.*

Proof: (i)⇒(ii) trivially, (iv)⇒(v) by 1.13, and (v)⇒(i) by 1.12.

(ii)⇒(iii): We have $1_S + d = 2_S + d$ for some $d \in S$. Then $1_S + c = c$, where $c = 1_S + d$.

(iii)⇒(iv): We have $a + ac = ac$. □

1.15 Lemma. *Assume that $0_S \in S$. Then the following conditions are equivalent:*

(i) $\rho_S = S \times S$;
(ii) $(a, 2a) \in \rho_S$ *for all* $a \in S$;
(iii) $(a, 0_S) \in \rho_S$ *for all* $a \in S$;
(iv) *for every* $a \in S$ *there exists* $b \in S$ *such that* $a + b = b$.

Proof: Use 1.12. □

1.16 Lemma. (i) Let I be an ideal of a semiring S such that I has a unit element 1_I. If S is generated by a set M, then I (as a semiring) is generated by the set $M1_I$. In particular, if S is finitely generated, then I is so.

(ii) Let S be a finitely generated semiring with a subsemiring $Q \cong \mathbb{Q}^+$. Then $S \cdot 1_Q$ is a finitely generated semiring with unit 1_Q containing a copy of $\mathbb{Q}^+$.

Proof: Easy to see. □

1.17 Lemma. *The semiring $\mathbb{Q}^+$ of positive rational numbers is congruence-simple.*

Proof: Let r be a congruence of $\mathbb{Q}^+$, $r \neq \mathrm{id}$. Then there are positive integers $m > n$ such that $(m, n) \in r$. Choose $k \in \mathbb{N}$ such that $m^k > 2n^k$. We have $(m^k, n^k) \in r$, and so $(m^k - n^k, 2(m^k - n^k)) = (n^k + (m^k - 2n^k), m^k + (m^k - 2n^k)) \in r$. Therefore $(1, 2) = ((m^k - n^k)(m^k - n^k)^{-1}, 2(m^k - n^k)(m^k - n^k)^{-1}) \in r$. Thus $(s, t) \in r$ for all $s, t \in \mathbb{Q}^+$, and so $r = \mathbb{Q}^+ \times \mathbb{Q}^+$. □

1.18 Proposition. *Let T be a finitely generated semiring such that $Q \simeq \mathbb{Q}^+$ is a subsemiring of T. Then T is not additively cancellative.*

Proof: Assume that T is additively cancellative and denote by R the Dorroh extension of the difference ring of T. R is a finitely generated ring, has a unit element and the field $\mathbb{Q}$ of rational numbers is isomorphic to a subring of R containing Q.

Let I be a maximal ideal of R. Since $\mathbb{Q}$ is a simple ring, we get either $Q \subseteq I$ or $Q \cap I = 0$. If $Q \cap I = 0$ then $\mathbb{Q}$ is isomorphic to a subring of R/I. But R/I is a finitely generated field, hence finite, a contradiction. Thus $Q \subseteq I$. Hence $1_Q \in Q \subseteq \bigcap_{I \in \mathrm{Max}(R)} I = J(R)$, a contradiction. □

1.19 Lemma. *Let S be a finitely generated semiring with unit containing a subsemiring $Q \simeq \mathbb{Q}^+$ such that $1_S \in Q$. Then $\rho_S = S \times S$.*

Proof: First, put $T = S/\rho_S$. Then T is a finitely generated additively cancellative semiring (and T is trivial if and only if $\rho_S = S \times S$). If $\rho_S \restriction Q = \mathrm{id}_Q$ then $\mathbb{Q}^+$ is isomorphic to a subsemiring of T, which is impossible by 1.18. Thus $\rho_S \restriction Q \neq \mathrm{id}_Q$.

$Q \simeq \mathbb{Q}^+$ is congruence-simple by 1.17, and so $\rho_S \restriction Q = Q \times Q$ and Q is contained in a block of ρ_S. Consequently, $1/\rho_S$ is an additively idempotent element of T and, since T is additively cancellative, it follows easily that $1/\rho_S$ is additively neutral and multiplicatively absorbing. Thus $a/\rho_S = (a \cdot 1)/\rho_S = a/\rho_S \cdot 1/\rho_S = 1/\rho_S$ for every $a \in S$ and $\rho_S = S \times S$. □

2. Parasemifields - introduction

By a *parasemifield* we mean a non-trivial semiring whose multiplicative semigroup is an (abelian) group.

2.1 Lemma. *Let S be a parasemifield. Then:*

(i) *$0_S \notin S$ and $1_S \in S$,*
(ii) *S is infinite,*
(iii) *S is ideal-free (i.e., S is the only ideal of S).*

Proof: The automorphism group of $S(+)$ is transitive and the rest is clear. □

2.2 Lemma. *Let S be a parasemifield.*

(i) *S is additively idempotent if and only if $1_S = 2_S$.*

(ii) *If S is not additively idempotent and P denotes the smallest subparasemifield of S (i.e., the subparasemifield generated by 1_S), then $P \simeq \mathbb{Q}^+$.*

Proof: (i) Easy to see.

(ii) P is a homomorphic image of $\mathbb{Q}^+$, i.e., $P \simeq \mathbb{Q}^+/r$ for a congruence r of $\mathbb{Q}^+$. But $\mathbb{Q}^+$ is congruence-simple by 1.17. If $r = \mathbb{Q}^+ \times \mathbb{Q}^+$ then P is trivial and S is additively idempotent. Thus $r = \mathrm{id}$ and $P \simeq \mathbb{Q}^+$. □

2.3 Remark. (i) Parasemifields together with trivial semirings form an equational class of universal algebras (two binary, one unary and one nullary operation).

(ii) If $\kappa \geq 2$ is a cardinal number then the parasemifield $(\mathbb{Q}^+)^\kappa$ is not congruence-simple.

2.4 Lemma. *A semiring S is a parasemifield if and only if S is ideal-free.*

Proof: If S is ideal-free then $Sa = S$ for every $a \in S$, and hence $S(\cdot)$ is a group. □

2.5 Remark. Let S be a parasemifield. Then $S(*, \cdot)$ is again a parasemifield, where $a * b = (a^{-1} + b^{-1})^{-1}$ for all $a, b \in S$ (the adjoint parasemifield).

The mapping $a \mapsto a^{-1}$ is an isomorphism of $S(+, \cdot)$ onto $S(*, \cdot)$ and vice versa.

2.6 Remark ([3]). There exists a one-to-one correspondence between additively idempotent parasemifields and lattice-ordered abelian groups. If S is an additively idempotent parasemifield, $a \wedge b = a + b$ and $a \vee b = (a^{-1} + b^{-1})^{-1}$ $(= a * b)$, then $S(\cdot, \wedge, \vee)$ is a lattice-ordered group. Conversely, if $S(\cdot, \wedge, \vee)$ is a lattice-ordered group and $a + b = a \wedge b$, then $S(+, \cdot)$ is an additively idempotent parasemifield.

2.7 Remark. Let S be a non-trivial multiplicatively cancellative semiring. Then there exists a parasemifield P (the parasemifield of fractions) such that $P = \{ab^{-1} \mid a, b \in S\}$. Moreover, P is additively idempotent (cancellative, resp.) if and only if S is so.

2.8 Lemma. *Let S be a parasemifield. Then the multiplicative group $S(\cdot)$ is torsionfree.*

Proof: Let $a \in S$ and $m \in \mathbb{N}$ be such that $a^m = 1$. Then $a(1+a+\dots+a^{m-1}) = a + a^2 + \dots + a^{m-1} + 1$, and therefore $a = 1$. □

3. The relations μ_S, ν_S, η_S, and ρ_S

Throughout this section, let S be a parasemifield.

3.1 Lemma. *If $a, b \in S$, $k \in \mathbb{N}$ are such that $(a^k, b^k) \in \mu_S$, then $(a, b) \in \mu_S$.*

Proof: We have $b^k = a^k + z$ for some $z \in S \cup \{0\}$. Let $x = a^{k-1} + a^{k-2}b + \dots + ab^{k-2} + b^{k-1}$. Then $bx = a^{k-1}b + a^{k-2}b^2 + \dots + ab^{k-1} + b^k = a^{k-1}b + a^{k-2}b^2 + \dots + ab^{k-1} + a^k + z = ax + z$, and so $b = a + zx^{-1}$ and $(a, b) \in \mu_S$. □

3.2 Lemma. *Let $r \in \mathbb{Q}^+$ and $k \in \mathbb{N}$ be such that $r^{k+1} < k+1$. Then $(r_S, a + a^{-k}) \in \mu_S$ for every $a \in S$.*

Proof: We have $(a + a^{-k})^{k+1} = a^{k+1} + (k+1)a^k a^{-k} + \dots = (k+1) + z$ for some $z \in S$, thus $((k+1)_S, (a + a^{-k})^{k+1}) \in \mu_S$. Further $(r_S^{k+1}, (k+1)1_S) \in \mu_S$, and so $(r_S^{k+1}, (a + a^{-k})^{k+1}) \in \mu_S$ and $(r_S, a + a^{-k}) \in \mu_S$ by 3.1. □

3.3 Corollary. *$(1_S, a + a^{-k}) \in \mu_S$ for all $a \in S$ and $k \in \mathbb{N}$.*

3.4 Lemma. *For all $n \in \mathbb{N}$,*

$$\lim_{m\to\infty} \binom{(n+1)m}{nm}^{1/(n+1)m} = \frac{n+1}{n} \cdot n^{1/(n+1)}.$$

Proof: Put $a_m = \binom{(n+1)m}{nm}$. Then

$$\begin{aligned}\lim_{m\to\infty} \frac{a_{m+1}}{a_m} &= \lim_{m\to\infty} \frac{((n+1)m+n+1)!(nm)!m!}{(nm+n)!(n+1)!((n+1)m)!} \\ &= \lim_{m\to\infty} \frac{((n+1)m+n+1)\dots((n+1)m+1)}{(nm+n)\dots(nm+1)(m+1)} = \frac{(n+1)^{n+1}}{n^n}.\end{aligned}$$

Using the well-known Cauchy criterion we get

$$\lim_{m\to\infty} a_m^{1/m} = \lim_{m\to\infty} \frac{a_{m+1}}{a_m} = \frac{(n+1)^{n+1}}{n^n}.$$

□

3.5 Remark. Denote $\frac{n+1}{n} \cdot n^{1/(n+1)} = f(n)$. Then $f(1) = 2$, $f(n) > f(n+1)$ and $\lim_{n\to\infty} f(n) = 1$. Also $f(n) > \binom{(n+1)m}{nm}^{1/(n+1)m}$ for all $m \in \mathbb{N}$. (Use the binomial formula for $f(n)^{(n+1)m} = (n^{1/(n+1)} + n^{-n/(n+1)})^{(n+1)m}$. The rest is easy.)

3.6 Lemma. *$((f(n)-r)_S, a+a^{-n}) \in \mu_S$ for all $n \in \mathbb{N}$, $a \in S$, $r \in \mathbb{Q}^+$, $r < f(n)$.*

Proof: Denote $f(n) - r = x$. There is a positive integer m such that $x^{(n+1)m} < \binom{(n+1)m}{nm}$ by 3.4 and 3.5. Using the binomial formula for $(a + a^{-n})^{(n+1)m}$ we see that $(\binom{(n+1)m}{nm}1_S, (a + a^{-n})^{(n+1)m}) \in \mu_S$. Consequently, $(x_S^{(n+1)m}, (a + a^{-n})^{(n+1)m}) \in \mu_S$ and therefore $(x_S, a + a^{-n}) \in \mu_S$ by 3.1. □

3.7 Lemma. *If $(a,b) \in \mu_S$ then $(b^{-1}, a^{-1}) \in \mu_S$.*

Proof: If $a + z = b$ then $a^{-1} = b^{-1} + z(ab)^{-1}$. □

3.8 Lemma. (i) *$(a(a^{n+1} + 1_S)^{-1}, 1_S) \in \mu_S$ for every $a \in S$, $n \in \mathbb{N}$.*

(ii) *$(a(a^{n+1} + 1_S)^{-1}, (f(n) - r)_S^{-1}) \in \mu_S$ for every $n \in \mathbb{N}$, $a \in S$, $r \in \mathbb{Q}^+$, $r < f(n)$.*

(iii) *$(a(a^2 + 1_S)^{-1}, n(2n-1)_S^{-1}) \in \mu_S$ for all $a \in S$, $n \in \mathbb{N}$.*

Proof: Use 3.3, 3.5, 3.6 and 3.7. □

3.9 Lemma. *$\nu_S \neq S \times S$.*

Proof: If $\nu_S = S \times S$ then S is a ring by 1.1(iii), a contradiction with $0 \notin S$.

□

3.10 Lemma. *The following conditions are equivalent for $a, b \in S$:*

(i) *$(a,b) \in \eta_S$;*

(ii) *$(a^{-1}b, 1_S) \in \eta_S$;*

(iii) *there exist $m, n \in \mathbb{N}$ such that $(m_S^{-1}, a^{-1}b) \in \mu_S$ and $(a^{-1}b, n_S^{-1}) \in \mu_S$;*

(iv) *there exist $r, s \in \mathbb{Q}^+$, $r < s$, such that $(r_S, a^{-1}b) \in \mu_S$ and $(a^{-1}b, s_S) \in \mu_S$;*

(v) *there exists $k \in \mathbb{N}$, such that $(2_S^{-k}, a^{-1}b) \in \mu_S$ and $(a^{-1}b, 2_S^k) \in \mu_S$.*

Proof: Easy to check. □

3.11 Proposition. (i) $\eta_S = \mathrm{id}_S$ *if and only if* S *is additively idempotent.*

(ii) $\eta_S = S \times S$ *if and only if* S *is additively archimedean (and then* S *is additively cancellative).*

(iii) *If* A *is a block of* η_S*, then* $A(+)$ *is a cancellative subsemigroup of* $S(+)$.

(iv) $(a, b) \in \eta_S$ *if and only if* $a^{-1}b \in P = \{c \,|\, (c, 1_S) \in \eta_S\}$.

(v) *Either* $P = \{1_S\}$ *(and then* S *is additively idempotent) or* P *is an additively cancellative archimedean subparasemifield of* S.

PROOF: For (i),(ii),(iii) and (iv) see 1.6, 1.8, 1.9 and 3.10.

(v) To show that P is additively archimedean, it is enough to prove that $(c, 1_S) \in \eta_P$ for every $c \in P$. Let $c + d = n1_S$ and $1_S + e = mc$, where $c \in P$, $d, e \in S$, $n, m \in \mathbb{N}$. Put $d' = d + 1_S$ and $e' = e + c$. Then $d' + c = (n + 1)1_S$, $1_S + d = d'$, $e' + (1_S + (m + 1)d) = (m + 1)n1_S$ and $1_S + (m + 1)e = me'$, hence $d', e' \in P$. Since $c + d' = (n + 1)1_S$ and $1_S + e' = (m + 1)c$, we get $(c, 1_S) \in \eta_P$.

The rest follows from 1.5(i) and 1.8. □

3.12 Lemma. $\eta_S = \nu_S$ *if and only if* $(2_S, 1_S) \in \mu_S$.

PROOF: Easy to see. □

3.13 Lemma. *The following conditions are equivalent:*

(i) $\rho_S = S \times S$;
(ii) $a + b = a$ *for some* $a, b \in S$;
(iii) $(1_S, 2_S) \in \rho_S$;
(iv) $c = c + 1_S$ *for some* $c \in S$;
(v) $1_S = 1_S + d$ *for some* $d \in S$;
(vi) *for all* $x \in S$ *there exists* $y \in S$ *such that* $x + y = x$.

PROOF: Easy (use 1.14). □

3.14 Proposition. (i) *If* S *is finitely generated as a semiring, then* S *is not additively cancellative and* S *satisfies the equivalent conditions of* 3.13.

(ii) *The additive semigroup* $S(+)$ *is not finitely generated.*

(iii) *If the multiplicative group* $S(\cdot)$ *has finite (Prüfer) rank, then* S *is additively idempotent.*

PROOF: (i) Use 1.12(ii), 2.2(ii), 1.18 and 1.19.

(ii) Suppose $S(+)$ is generated by $\{a_1, \dots, a_n\}$. If S is additively idempotent then S is finite, a contradiction with 2.1. Hence $\rho_S = S \times S$ by 2.2 and 1.19. There are $b_i \in S$, $i = 1, \dots, n$ such that $a_i + b_i = b_i$, by 1.14. Thus $ka_i + b_i = b_i$ for every $k \in \mathbb{N} \cup \{0\}$ and $i = 1, \dots, n$. Put $o = \sum_i b_i$. Then for every $x = \sum_i k_i a_i \in S$, $k_i \in \mathbb{N} \cup \{0\}$, we get $x + o = o$. Hence $o + o = o$, a contradiction with $\mathbb{Q}^+ \subseteq S$.

(iii) The multiplicative group $\mathbb{Q}^+(\cdot)$ is a free abelian group of infinite rank.

□

4. More results on parasemifields

In this section, let S be a parasemifield that is not additively idempotent. According to 2.2(ii), the prime subparasemifield of S is a copy of $\mathbb{Q}^+$ and (without loss of generality) we can assume that it is equal to $\mathbb{Q}^+$.

Put $P = \{a \in S \,|\, (a,1) \in \eta_S\}$, $Q = \{a \in S \,|\, (a,r) \in \mu_S$ for some $r \in \mathbb{Q}^+\}$, $R = \{a \in S \,|\, (r,a) \in \mu_S$ for some $r \in \mathbb{Q}^+\}$. According to 3.11(v), P is additively cancellative archimedean subparasemifield of S.

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

(i) *$a \in P$;*
(ii) *$a^{-1} \in P$;*
(iii) *there exist $m, n \in \mathbb{N}$ such that $(m_S^{-1}, a) \in \mu_S$ and $(a, n_S^{-1}) \in \mu_S$;*
(iv) *there exist $r, s \in \mathbb{Q}^+$, $r < s$, such that $(r_S, a) \in \mu_S$ and $(a, s_S) \in \mu_S$;*
(v) *there exists $k \in \mathbb{N}$, such that $(2_S^{-k}, a) \in \mu_S$ and $(a, 2_S^k) \in \mu_S$;*
(vi) *$a \in Q \cap R$.*

Proof: See 3.10. □

4.2 Lemma. *Let $a, b, c \in S$. If $(a,b) \in \mu_S$, $(b,c) \in \mu_S$ and $a, c \in P$, then $b \in P$.*

Proof: Use 4.1. □

4.3 Proposition. (i) *Both Q and R are subsemirings of S.*
(ii) *$Q \cap R = P$.*
(iii) *$a \in Q$ if and only if $a^{-1} \in R$ (i.e., $R = Q^{-1}$).*

Proof: Easy (use 4.1). □

4.4 Lemma. *If $a_1, \dots, a_m \in S$, $m \in \mathbb{N}$ are such that $a_1 + \dots + a_m \in Q$, then $a_1, \dots, a_m \in Q$.*

Proof: Obvious. □

4.5 Lemma. *$R + S \subseteq R$ (i.e., R is an ideal of $S(+)$).*

Proof: Obvious. □

4.6 Lemma. *Let $a \in S$, $k \in \mathbb{N}$. Then*

(i) *$a \in Q$ if and only if $a^k \in Q$,*
(ii) *$a \in R$ if and only if $a^k \in R$,*
(iii) *$a \in P$ if and only if $a^k \in P$.*

Proof: (i) If $a^k \in Q$ then $(a^k, r) \in \mu_S$ for some $r \in \mathbb{Q}^+$. We have $r < s^k$ for some $s \in \mathbb{Q}^+$ and $(a^k, s^k) \in \mu_S$. Then $(a,s) \in \mu_S$ by 3.1, and so $a \in Q$.

(ii) Similar to (i).

(iii) Combine (i), (ii) and 4.3(ii). □

Let $a \in S$. Denote K_a the subsemiring of S generated by $\mathbb{Q}^+ \cup \{a\}$. Clearly, K_a is the set of elements of the form $r_0 + r_1a + r_2a^2 + \dots + r_ma^m$, $m \geq 0$, $r_i \in \mathbb{Q}^+ \cup \{0\}$, $\sum r_i \neq 0$.

4.7 Lemma. *Let $a \in S$, $k \in \mathbb{N}$, $g \in K_a$. Then:*

(i) $a + 1, (a+1)a^{-1}, (a^k+1)a^{-1}, a + a^{-k} \in R$;

(ii) $(a+1)^{-1}, a(a+1)^{-1}, a(a^k+1)^{-1}, a^k(a^{k+1}+1)^{-1} \in Q$;

(iii) $g + a^{-1} \in R$;

(iv) $a(ag+1)^{-1} \in Q$.

Proof: (i) We have $(1, a+1) \in \mu_S$ and $(1, a^{-1}+1) = (1, (a+1)a^{-1}) \in \mu_S$. Thus $a+1, (a+1)a^{-1} \in R$. Further, $a^{-1} + (a^{-1})^{-(k-1)} = (a^k+1)a^{-1} \in R$ and $a + a^{-k} \in R$ by 3.3.

(iii) Let $g = \sum_{i \in I} r_i a^i$, I is a finite non-empty subset of $\mathbb{N} \cup \{0\}$, $r_i \in \mathbb{Q}^+, i \in I$. Fix arbitrary $j \in I$. $(a^{j+1}+1)a^{-1} = a^j + a^{-1} \in R$ by (i). Let $r = \min(1, r_j)$. Then $(r(a^j + a^{-1}), r_ja^j + a^{-1}) \in \mu_S$, and so $r_ja^j + a^{-1} \in R$. Then $g + a^{-1} = r\sum_{i \in I \setminus \{j\}} r_ia^i + (r_ja^j + a^{-1}) \in R$ by 4.5.

(ii), (iv) Use (i), (iii) and 4.3(iii). □

4.8 Proposition. $QQ^{-1} = S = RR^{-1} (= QR = RQ)$.

Proof: By 4.7, $a(a+1)^{-1} \in Q$ and $a+1 \in Q^{-1} = R$ for each $a \in S$. Thus $a \in QQ^{-1}$. □

4.9 Corollary. *The following conditions are equivalent:*

(i) $Q = S$ *($R = S$, resp.);*

(ii) $Q = P$ *($R = P$, resp.);*

(iii) Q *(R, resp.) is a parasemifield;*

(iv) $P = S$;

(v) $P = Q = R = S$.

4.10 Proposition. $Q + \mathbb{Q}^+ = P$.

Proof: We have $\mathbb{Q}^+ \subseteq P \subseteq Q$, Q is a semiring, and so $Q + \mathbb{Q}^+ \subseteq Q$. Clearly, $Q + \mathbb{Q}^+ \subseteq R$ by the definition of R. Thus $Q + \mathbb{Q}^+ \subseteq Q \cap R = P$.

On the other hand, if $a \in P$ then $a = r + z$ for $r \in \mathbb{Q}^+$, $z \in S \cup \{0\}$ (because $a \in R$). Put $v = r/2 + z$. We have $a \in Q$, $(v, a) \in \mu_S$, and so $v \in Q$ by the definition of Q. Hence $a = v + r/2 \in Q + \mathbb{Q}^+$. □

4.11 Corollary. $(ra+1)a^{-1} \in P$ *for all* $a \in R$, $r \in \mathbb{Q}^+$.

4.12 Lemma. *Let $a \in S$, $k \in \mathbb{N}$, $g \in K_a$. Then the elements* $(a+1)(a+2)^{-1}$, $(a+2)(a+1)^{-1}$, $(a^k+a+1)(a^k+1)^{-1}$, $(a^k+1)(a^k+a+1)^{-1}$, $(a^{k+1}+a^k+1)(a^{k+1}+1)^{-1}$, $(a^{k+1}+1)(a^{k+1}+a^k+1)^{-1}$, $(ag+a+1)(ag+1)^{-1}$, $(ag+1)(ag+a+1)^{-1}$ *are in P.*

Proof: By 4.7(ii), $(a+1)^{-1} \in Q$, and hence $(a+2)(a+1)^{-1} = (a+1)^{-1}+1 \in P$ by 4.10. The rest is similar. □

4.13 Lemma. *Let $a, b \in P$ and $c \in S$ be such that $b + a = c + a$. Then $b + b = c + b$.*

Proof: $(a, b) \in \eta_S$, and so $a + d = 2^m b$ for some $d \in S$ and $m \in \mathbb{N}$. Then $b + 2^m b = c + 2^m b$ (see the proof of 1.8), and so $b + b = c + b$ by 1.7. □

4.14 Lemma. *Let $e \in S$ be such that $1 + e = 1$. Then:*

(i) *$e \in Q, e \notin P$;*

(ii) *$a + e = a$ for all $a \in P$;*

(iii) *$a + be = a$ for all $a, b \in P$.*

Proof: Clearly $e \in Q$. From $a/2 + e + 1 = a/2 + 1$ for all $a \in P$ it follows that $a + e = a$ by 4.13. Consequently, $ab + be = ab$ for all $a, b \in P$, thus $c + be = c$ for all $b, c \in P$.

If $e \in P$ then $e + e = e$, and so $2 = 1$, a contradiction. □

4.15 Lemma. *Let $a, b, c \in Q$ be such that $a + b = a + c$. Then $b + r = c + r$ for all $r \in \mathbb{Q}^+$.*

Proof: We have $a' = a + r \in P$, $b' = b + r \in P$, $c' = c + r \in P$ by 4.10. Since $a' + b' = a' + c'$ and P is additively cancellative, we get $b' = c'$. □

4.16 Corollary. *Let $b, c \in Q$. Then $(b, c) \in \rho_Q$ if and only if $b + r = c + r$ for all $r \in \mathbb{Q}^+$.*

4.17 Proposition. *$\rho_Q \restriction P = \mathrm{id}_P$. In particular, $\rho_Q \neq Q \times Q$.*

Proof: If $b, c \in P$ are such that $(b, c) \in \rho_Q$, then $b + 1 = c + 1$ by 4.16. Then $b = c$ by 3.11(v). □

4.18 Proposition. *The semiring Q is not finitely generated.*

Proof: The result follows as an immediate consequence of 1.19 and 4.17. □

4.19 Remark. Assume that the semiring S is generated by a finite set $\{x_1, \dots, x_m\}$ of its elements ($m \in \mathbb{N}$).

(i) $\mathbb{N}_0^m$ is clearly a subsemigroup of the cartesian power $\mathbb{Z}^m$ and the additive semigroup $S(+)$ is generated by the set $\{x_1^{k_1} \cdots x_m^{k_m} \mid (k_1, \dots, k_m) \in \mathbb{N}_0^m\}$.

(ii) Put $N = \{(l_1, \dots, l_m) \in \mathbb{N}_0^m \mid x_1^{l_1} \cdots x_m^{l_m} \in Q\}$. From 4.4 it follows easily that $N \neq \emptyset$ and that the additive semigroup $Q(+)$ is generated by the set $\{x_1^{l_1} \cdots x_m^{l_m} \mid (l_1, \dots, l_m) \in N\}$.

(iii) Clearly, $N(+)$ is a subsemigroup of $\mathbb{N}_0^m(+)$. If $N(+)$ were a finitely generated semigroup, Q would be a finitely generated semiring, a contradiction with 4.18. Thus $N(+)$ is not a finitely generated semigroup.

(iv) It follows easily from (iii) that $m \geq 2$. Moreover, if $m = 2$ then $x_1 \neq x_2^u$, $x_2 \neq x_1^v$, $u, v \in \mathbb{Z}$ (in particular, $x_1 \neq x_2^{-1}$).

4.20 Remark. Let $a \in S$. Put $Q_a = Q \cap K_a$ (K_a denotes the subsemiring of S generated by $\mathbb{Q}^+ \cup \{a\}$). Denote $M = \{k \in \mathbb{N}_0 \,|\, a^k \in Q_a\}$. Then M is a subsemigroup of $\mathbb{Z}(+)$ and $M = \{0\}$ if and only if $Q_a = \mathbb{Q}^+$ and $a \notin \mathbb{Q}^+$(use 4.4 and 4.6(i)).

(i) Assume that $M \neq \{0\}$. If l is the smallest positive integer in M, then $l = 1$ by 4.6(i), and so $M = \mathbb{N}_0$. Then $Q_a = K_a$ by 4.4.

(ii) Assume that $a^{-n} \in K_a$ for some $n \in \mathbb{N}$. Then $a^{-n} = \sum r_i a^i$, therefore $\sum r_i a^{i+n} = 1 \in Q$, and $a \in Q$ by 4.4 and 4.6(i). Hence $a^{-1} = \sum r_i a^{i+n-1} \in Q$ and $a \in Q^{-1} = R$. Thus $a \in Q \cap R = P$ and $Q_a \subseteq K_a \subseteq P$.

4.21 Theorem. *Let S be a parasemifield, $\mathbb{Q}^+ \leq S$ a subparasemifield and $a \in S$. If S is generated by $\mathbb{Q}^+ \cup \{a\}$ as a semiring, then the semiring S is not finitely generated.*

Proof: By the notation of 4.20 we have $K_a = S$. Then $a^{-1} \in K_a$, and so $K_a \subseteq P$ by 4.20(ii). Consequently, $P = S$ and so S is additively cancellative. By 1.18 the semiring S is not finitely generated. □

4.22 Remark. Every non-trivial finitely generated algebraic system has at least one maximal congruence. Combining this well known fact with 3.14(i) and [1, 10.1], one concludes easily that in fact, no parasemifield is a one-generated semiring. On the other hand, the parasemifield $\mathbb{Z}(\oplus, *)$, where $m \oplus n = \min(m, n)$ and $m * n = m + n$ for all $m, n \in \mathbb{Z}$, is a two generated semiring (it is generated by the two-element set $\{1, -1\}$). Of course, this parasemifield is additively idempotent.

The results of 4.21 and 4.22 lead us to the following conjectures:

(a) Let S be a parasemifield that contains $\mathbb{Q}^+$ as a subparasemifield and $K \subseteq S$ be a finite set. If S is generated by $\mathbb{Q}^+ \cup K$ as a semiring, then the semiring S is not finitely generated.

(b) Every parasemifield that is finitely generated as a semiring is additively idempotent.

Actually, it is easy to see (using 2.2) that (a) and (b) are equivalent.

Acknowledgment. The authors express their thanks to Robert El Bashir for his careful reading and useful comments, especially for the suggestion of Remark 4.22.

References

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

[2] Kala V., Kepka T., *A note on finitely generated ideal-simple commutative semirings*, Comment. Math. Univ. Carolin. **49** (2008), 1–9.

[3] Weinert H.J., Wiegandt R., *On the structure of semifields and lattice-ordered groups*, Period. Math. Hungar. **32** (1996), 147–162.

Charles University, Faculty of Mathematics and Physics, Department of Algebra,
Sokolovská 83, 186 75 Prague 8, Czech Republic

E-mail: vita211@gmail.com
kepka@karlin.mff.cuni.cz
miroslav.korbelar@gmail.com

(*Received* September 15, 2008, *revised* July 7, 2009)