Acta Universitatis Carolinae. Mathematica et Physica

Tomáš Kepka; Miroslav Korbelář
Various examples of parasemifields

*Acta Universitatis Carolinae. Mathematica et Physica*, Vol. 50 (2009), No. 1, 61--72

Persistent URL: http://dml.cz/dmlcz/142780

# Various Examples of Parasemifields

TOMÁŠ KEPKA and MIROSLAV KORBELÁŘ

Praha

*Received 15. October 2008*

We find an equivalent condition under which is the semiring $\mathbb{Q}^+[\alpha]$, $\alpha \in \mathbb{C}$, contained in a parasemifield of $\mathbb{C}$. A classification for the case when $\alpha$ is algebraic of degree 2 is made. Various examples of parasemifields are constructed.

## 1. Introduction

A (commutative) *semiring* is an algebraic structure with two commutative and associative binary operations (an addition and a multiplication) such that the multiplication distributes over the addition. A (commutative) *parasemifield* is a semiring where the multiplicative part is a group. There was proved in [1] that the problem of showing that

(a) Every infinitely generated ideal-simple commutative semiring is additively idempotent,

is equivalent to the question that

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

By [2, 2.2], a parasemifield that is not additively idempotent contains a copy of the parasemifield $\mathbb{Q}^+$. Reformulating the conjecture from (b), we get that

Department of Algebra MFF UK, Sokolovská 83 186 75 Praha 8, Czech Republic

*2000 Mathematics Subject Classification.* 16Y60

*Key words and phrases.* Parasemifield.

This work is a part of the research project MSM00210839 financed by MŠMT. The first author was supported by the Grant Agency of Czech Republic, No. 201/09/0296.

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

(c) Every (commutative) parasemifield that contains a copy of $\mathbb{Q}^+$ is not finitely generated as a semiring.

In context of (c) we can naturally ask about the structure of parasemifields that contain a copy $Q$ of $\mathbb{Q}^+$ and are (as semirings) generated by $Q \cup K$ where $K$ is a finite set. Of course, $\mathbb{Q}^+$ is an easy example of such a parasemifield.

In this paper we find other examples of such parasemifields.

Another interesting problem is to describe all parasemifields that are contained in the field $\mathbb{C}$ of complex numbers. As we know, they must contain a copy of $\mathbb{Q}^+$. In this paper we characterize the case when $\mathbb{Q}^+[\alpha] \subseteq \mathbb{C}$ is a parasemifield, where $\alpha \in \mathbb{C}$ is algebraic of degree 2 over $\mathbb{Q}$.

## 2. Preliminaries

The following notation will be used in the sequel:

$\mathbb{N}$ ... the semiring of positive integers;
$\mathbb{N}_0$ ... the semiring of non-negative integers;
$\mathbb{Z}$ ... the ring of integers;
$\mathbb{Q}$ ... the field of rationals;
$\mathbb{Q}^+$ ... the parasemifield of positive rationals;
$\mathbb{Q}_0^+$ ... the semifield of non-negative rationals;
$\mathbb{Q}^-$ ... the set of negative rationals;
$\mathbb{R}$ ... the field of reals;
$\mathbb{R}^+$ ... the parasemifield of positive reals;
$\mathbb{R}_0^+$ ... the semifield of non-negative reals;
$\mathbb{R}^-$ ... the set of negative reals;
$\mathbb{R}_0^-$ ... the set of non-negative reals;
$\mathbb{C}$ ... the field of complex numbers.

## 3. Auxiliary results (a)

Put $s(a,n) = \binom{2n}{n}a^n$ for all $a \in \mathbb{R}$ and $n \in \mathbb{N}_0$.

**Lemma 3.1** (i) $s(a,0) = 1$, $s(a,1) = 2a$, $s(a,2) = 6a^2$, $s(a,3) = 20a^3$.
(ii) *If $a = 0$, then $s(a,k) = 0$ for every $k \geq 1$.*
(iii) *If $a \in \mathbb{R}^+$, then $s(a,n) \in \mathbb{R}^+$ for every $n$.*
(iv) *If $a \in \mathbb{R}^-$, then $s(a,n) \in \mathbb{R}^+$ for $n$ even and $s(a,n) \in \mathbb{R}^-$ for $n$ odd.*

*Proof.* It is obvious. □

In the rest of this section, assume that $a \neq 0$ and put $t(a,n) = s(a,n+1)/s(a,n)$ for every $n \in \mathbb{N}_0$.

**Lemma 3.2** $t(a,n) = (4 - 2/(n+1))a$.

*Proof.* Easy to check. $\square$

**Lemma 3.3** $\lim_{n\to\infty} t(a,n) = 4a$.

*Proof.* The assertion follows easily from 3.2. $\square$

**Lemma 3.4** *If* $|a| \le 1/4$, *then* $\lim s(a,n) = 0$.

*Proof.* For $a = 0$ is the statement clear. Let $0 < |a| < 1/4$. By 3.3, we have $\lim |s(a,n+1)|/|s(a,n)| = \lim |t(a,n)| = 4|a| < 1$, hence $\lim s(a,n) = 0$.

Suppose now, $|a| = 1/4$. Then, using the Stirling's formula, $\lim \alpha_n/n! = 1$, where $\alpha_n = (n/e)^n \sqrt{2\pi n}$, we get $\lim |s(a,n)| = \lim ((2n)!/\alpha_{2n})(\alpha_n/n!)^2(1/\sqrt{\pi n}) = 0$. $\square$

**Lemma 3.5** *If* $|a| > 1/4$, *then* $\lim |s(a,n)| = \infty$.

*Proof.* By 3.3, there are $n_0 \in \mathbb{N}_0$ and $r \in \mathbb{R}$ such that $r > 1$ and $|t(a,k)| \ge r$ for every $k \ge n_0$. Now, $|s(a,k)| \ge r^{k-n_0} \cdot |s(a,n_0)|$ for $k \ge n_0$ and the rest is clear. $\square$

**Lemma 3.6** *(i) If* $a > 1/4$, *then* $\lim s(a,n) = +\infty$.
*(ii) If* $a < -1/4$, *then* $\lim s(a,n)$ *does not exist.*

*Proof.* Combine 3.5 and 3.1(iii),(iv). $\square$

## 4. Auxiliary results (b)

Put $\mathbf{h}(n,a,b) = (x+1)\prod_{i=0}^{n}((x^2+b)^{2^i} + (ax)^{2^i}) \in \mathbb{R}[x]$ for all $a, b \in \mathbb{R}$ and $n \in \mathbb{N}_0$.

**Lemma 4.1** $\mathbf{h}(n,a,b)$ *is a monic polynomial of degree* $2^{n+2} - 1$.

*Proof.* It is obvious. $\square$

Put $\mathbf{g}(n,a,b,c,d) = (x^2 + b - ax)\mathbf{h}(n,c,d) \in \mathbb{R}[x]$ for all $a,b,c,d \in \mathbb{R}$ and $n \in \mathbb{N}_0$.

**Lemma 4.2** $\mathbf{g}(n,a,b,c,d)$ *is a monic polynomial of degree* $2^{n+2} + 1$.

*Proof.* Is is obvious. $\square$

Put $\mathbf{f}(n,a,b) = \mathbf{g}(n,a,b,a,b)$.

**Lemma 4.3** $\mathbf{f}(n,a,b) = (x+1)((x^2+b)^{2^{n+1}} - (ax)^{2^{n+1}})$ *is a monic polynomial of degree* $2^{n+2} + 1$.

*Proof.* Put $f = x^2 + b$ and $g = ax$. Then $\mathbf{f}(n,a,b) = (x+1)(f-g)(f+g)(f^2+g^2)(f^4+g^4)\dots(f^{2^n}+g^{2^n}) = (x+1)(f^2-g^2)(f^2+g^2)(f^4+g^4)\dots(f^{2^n}+g^{2^n}) = (x+1)(f^4-g^4)(f^4+g^4)\dots(f^{2^n}+g^{2^n}) = \dots = (x+1)(f^{2^n}-g^{2^n})(f^{2^n}+g^{2^n}) = (x+1)(f^{2^{n+1}} - g^{2^{n+1}})$. $\square$

Let $\mathbf{f}(n,a,b) = \sum_{k=0}^{\infty} r_k(n,a,b)x^k \in \mathbb{R}[x]$, where $r_k(n,a,b) \in \mathbb{R}$.

**Lemma 4.4** (i) $r_k(n,a,b) = 0$ *for every* $k \geq 2^{n+2}+2$.

(ii) $r_k(n,a,b) = r_{k+1}(n,a,b) = \binom{2^{n+1}}{k/2} b^{2^{n+1}-k/2}$ *for every even* $k$, $0 \leq k \leq 2^{n+2}$, $k \neq 2^{n+1}$.

(iii) $r_{2^{n+1}}(n,a,b) = r_{2^{n+1}+1}(n,a,b) = \binom{2^{n+1}}{2^n} b^{2^n} - a^{2^{n+1}}$.

*Proof.* Combine 4.3 and the binomial formula. □

**Lemma 4.5** (i) *If* $b \geq 0$, *then* $r_k(n,a,b) \geq 0$ *for every* $k \in \mathbb{N}_0$ *such that* $k \neq 2^{n+1}$ *and* $k \neq 2^{n+1}+1$.

(ii) *If* $b > 0$, *then* $r_k(n,a,b) > 0$ *for every* $k \in \mathbb{N}_0$ *such that* $k \leq 2^{n+2}+1$, $k \neq 2^{n+1}$ *and* $k \neq 2^{n+1}+1$.

*Proof.* The assertion follows immediately from 4.4. □

**Lemma 4.6** *Assume that* $b > 0$ *(*$b \geq 0$*, resp.). Then the following conditions are equivalent:*

(i) $\binom{2^{n+1}}{2^n} b^{2^n} > a^{2^{n+1}}$ $\left(\binom{2^{n+1}}{2^n} b^{2^n} \geq a^{2^{n+1}}\right.$*, resp.*$\left.\right)$.

(ii) $r_k(n,a,b) > 0$ *(*$r_k(n,a,b) \geq 0$*, resp.) for every* $0 \leq k \leq 2^{n+2}+1$.

*Moreover, if* $a \neq 0$*, then these conditions are equivalent to*

(iii) $\binom{2^{n+1}}{2^n} (b/a^2)^{2^n} > 1$ *(*$\geq 1$*, resp.).*

*Proof.* Combine 4.5 and 4.4(ii),(iii). □

**Lemma 4.7** *If* $4b > a^2 > 0$*, then there is* $m \in \mathbb{N}$ *such that* $r_k(m,a,b) > 0$ *for every* $0 \leq k \leq 2^{m+2}+1$.

*Proof.* We have $b/a^2 > 1/4$, and hence $\lim s(b/a^2, n) = +\infty$ by 3.6(i). Consequently, there is $k \in \mathbb{N}_0$ such that $s(b/a^2, l) > 1$ for every $l \geq k$. Now, it suffices to find $m \in \mathbb{N}$ with $2^m \geq k$ and our result follows from 4.6. □

**Lemma 4.8** *Assume that* $4b > a^2 > 0$*. Then there exist* $m \in \mathbb{N}$ *and* $c, d \in \mathbb{Q}$ *such that* $\mathbf{g}(m,a,b,c,d) \in \mathbb{R}^+[x]$.

*Proof.* First, let $\mathbf{g}(n,a,b,u,v) = \sum_{k=0}^{\infty} s_k(n,a,b,u,v)x^k \in \mathbb{R}[x]$, where $s_k(n,a,b,u,v) \in \mathbb{R}$. Clearly, $s_k(n,a,b,\cdot,\cdot) : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is a polynomial function and $s_k(n,a,b,a,b) = r_k(n,a,b)$, $s_l(n,a,b,u,v) = 0$ for every $a,b,u,v \in \mathbb{R}$, $n \in \mathbb{N}$, $0 \leq k \leq 2^{n+2}+1$ and $l \geq 2^{n+2}+2$.

Now, by 4.7, there are $m \in \mathbb{N}$ and $0 < r \in \mathbb{R}$ such that $s_k(m,a,b,a,b) = r_k(m,a,b) > r$ for every $0 \leq k \leq 2^{m+2}+1$. Since the functions $s_k(m,a,b,\cdot,\cdot)$ are continuous, there are $c, d \in \mathbb{Q}$ such that $s_k(m,a,b,c,d) > 0$ for every $0 \leq k \leq 2^{m+2}+1$. It follows that $\mathbf{g}(m,a,b,c,d) \in \mathbb{R}^+[x]$. □

## 5. Auxiliary results (c)

**Lemma 5.1** *Let $f \in \mathbb{R}[x]$ be a monic irreducible polynomial such that $f$ has no positive root in $\mathbb{R}$. Then there exists $h \in \mathbb{Q}[x]$ such that $h \neq 0$ and all the coefficients of the product $hf$ are non-negative.*

*Proof.* We have $\deg(f) \in \{1, 2\}$. If $f = x + a$, $a \in \mathbb{R}$, then $a \geq 0$ and we put $h = 1$. If $f = x^2 + ax + b$, $a, b \in \mathbb{R}$, then $f$ has no real roots at all, and it follows that $b > a^2/4$. In particular, $b > 0$ and we put $h = 1$ for $a \geq 0$. Anyway, if $a \neq 0$, then $\mathbf{g}(m, a, b, c, d) \in \mathbb{R}^+[x]$ for some $m \in \mathbb{N}$ and $c, d \in \mathbb{Q}$, by 4.8, and we put $h = \mathbf{h}(m, c, d) \in \mathbb{Q}[x]$ (see 4.1 and 4.2). □

**Lemma 5.2** *Let $f \in \mathbb{R}[x]$ be a polynomial such that $f$ has no positive real root. Then there exists $h \in \mathbb{Q}[x]$ such that $h \neq 0$ and all the coefficients of the product $hf$ are non-negative.*

*Proof.* We have $f = af_1 \cdots f_n$, where $a \in \mathbb{R}$, $n \in \mathbb{N}_0$ and $f_1, \dots, f_n$ are monic irreducible polynomials from $\mathbb{R}[x]$. By 5.1, there are non-zero polynomials $h_1, \dots, h_n \in \mathbb{Q}[x]$ such that all the products $h_i f_i$ belong to $\mathbb{R}_0^+[x]$. Now, it is enough to put $h = h_1 \cdots h_n$ for $a \geq 0$ and $h = -h_1 \cdots h_n$ for $a < 0$. □

**Proposition 5.3** *Let $F$ be a subfield of $\mathbb{R}$. The following conditions are equivalent for a non-zero polynomial $f \in F[x]$:*

(i) *The polynomial $f$ has no positive real root.*
(ii) *There exists a (non-zero) polynomial $h \in \mathbb{Q}[x]$ such that $hf \in F^+[x]$.*
(iii) *There exists a (non-zero) polynomial $g \in F^+[x]$ such that $f$ divides $g$ in $F[x]$.*

*Proof.* (i) implies (ii). By 5.2, there is $h \in \mathbb{Q}[x]$ such that $h \neq 0$ and $hf \in \mathbb{R}_0^+$. Clearly, $hf \neq 0$, $hf \in F[x]$, and therefore $hf \in F^+[x]$.

(ii) implies (iii). Put $g = hf$.

(iii) implies (i). We have $g = a_0 + a_1 x + \cdots + a_n x^n$, where $n \in \mathbb{N}_0, a_i \in F_0^+$ and $a_n \neq 0$. Now, if $r \in \mathbb{R}$ is such that $f(r) = 0$, then $\deg(f) \geq 1$, and hence $n \geq 1$ and $a_0 + a_1 r + \cdots + a_n r^n = 0$. It follows easily that $r \leq 0$. □

**Corollary 5.4** *A non-zero polynomial $f \in \mathbb{Q}[x]$ has no positive real root if and only if $f$ divides (in $\mathbb{Q}[x]$) a polynomial from $\mathbb{Q}^+[x]$.*

**Remark 5.5** Denote by $\mathfrak{A}$ the set of algebraic complex numbers $\alpha$ such that $f(\alpha) \neq 0$ for every $f \in \mathbb{Q}^+[x]$ ($\mathbb{N}[x]$, resp.) Then $\alpha \in \mathfrak{A}$ if and only if the minimal polynomial of $\alpha$ over $\mathbb{Q}$ has a positive real root.

**Remark 5.6** Let $\alpha \in \mathbb{C}$ be algebraic and let $f = \min_{\mathbb{Q}}(\alpha) \in \mathbb{Q}[x]$ ($f$ is a monic irreducible polynomial in $\mathbb{Q}[x]$).

(i) If $f$ has no positive real root then there is $g \in \mathbb{Q}^+[x]$ such that $g(\alpha) = 0$ (see 5.4). We have $g = q_0 + q_1 x + \cdots + q_n x^n$, where $n \in \mathbb{N}$, $q_i \in \mathbb{Q}_0^+$, $q_n \neq 0$ and $q_0 + q_1 \alpha + \cdots + q_n \alpha^n = 0$ (we can assume, without loss of generality, that $q_n = 1$ or that $q_i \in \mathbb{N}_0$).

(ii) If $\deg(f) = 1$, then $f = x - \alpha$ and $f$ has no positive real root iff $\alpha \notin \mathbb{R}^+$.

(iii) If $\deg(f) = 2$, then $f = (x - \alpha)(x - \beta)$ and $f$ has no positive real root iff $\alpha, \beta \notin \mathbb{R}^+$.

**Remark 5.7** (cf. 5.6) Let $\alpha \in \mathbb{C}$ be algebraic of degree 2 and such that the minimal polynomial $f = \min_{\mathbb{Q}}(\alpha)$ has a positive real root. Then $f = (x-\alpha)(x-\beta)$, $\alpha, \beta \in \mathbb{R}$, and either $\alpha \in \mathbb{R}^+$ or $\beta \in \mathbb{R}^+$. Furthermore, there are $q \in \mathbb{Q}^+$ and $t \in \mathbb{Q}$ such that just one of the following four cases takes place:

(1) $\alpha = \sqrt{q} + t > 0, \beta = -\sqrt{q} + t > 0$;
(2) $\alpha = \sqrt{q} + t > 0, \beta = -\sqrt{q} + t \leq 0$;
(3) $\alpha = -\sqrt{q} + t > 0, \beta = \sqrt{q} + t > 0$;
(4) $\alpha = -\sqrt{q} + t \leq 0, \beta = \sqrt{q} + t > 0$.

**Lemma 5.8** *Let $\alpha \in \mathbb{C}$ be algebraic of degree 2. Then the minimal polynomial $\min_{\mathbb{Q}}(\alpha)$ has a positive real root if and only if there exist $q \in \mathbb{Q}^+$ and $t \in \mathbb{Q}$ such that $\sqrt{q} > -t$, $\sqrt{q} \notin \mathbb{Q}$ and either $\alpha = t + \sqrt{q}$ or $\alpha = t - \sqrt{q}$.*

*Proof.* Easy (see 5.7). □

## 6. Auxiliary results (d)

In this section, let $q \in \mathbb{Q}^+$ be such that $\sqrt{q} \notin \mathbb{Q}$ ($\sqrt{q} \in \mathbb{R}^+$). Furthermore, let $t \in \mathbb{Q}$, $q_1 = \sqrt{q} + t$, $q_2 = -\sqrt{q} + t$, $A = \mathbb{Q}^+[q_1]$ $(= \{f(q_1) | f \in \mathbb{Q}^+[x]\})$ and $B = \mathbb{Q}^+[q_2]$.

**Lemma 6.1** *Both A and B are subsemirings of the field $\mathbb{R}$.*

*Proof.* Easy to see. □

**Proposition 6.2** *The following conditions are equivalent:*

(i) $\sqrt{q} > -t$.
(ii) $0 \notin A$.
(iii) $0 \notin B$.

*Proof.* Put $f = \min_{\mathbb{Q}}(q_1)$ $(= x^2 - 2tx + t^2 - q)$. Then $0 \in A$ iff $f$ divides a polynomial $g \in \mathbb{Q}^+[x]$ and the rest follows from 5.4 and 5.8. □

**Lemma 6.3** (i) $\mathbb{Q}^+[\sqrt{q}] = \{a + b\sqrt{q} | a, b \in \mathbb{Q}_0^+, a + b \neq 0\}$ *is a subsemiring of* $\mathbb{R}^+$.

(ii) $\mathbb{Q}^+[\sqrt{q}]^* = \{a, a\sqrt{q} | a \in \mathbb{Q}^+\}$ (*the group of invertible elements of the semiring* $\mathbb{Q}^+[\sqrt{q}]$).

*Proof.* (i) Easy to see.

(ii) Let $a + b\sqrt{q} \in \mathbb{Q}^+[\sqrt{q}]^*$, $a, b \in \mathbb{Q}^+$, $a + b \neq 0$. Of course, $(a + b\sqrt{q})^{-1} = a/c + (-b/c)\sqrt{q}$, $c = a^2 - b^2 q$. Consequently, if $a/c \neq 0$ then $c > 0$ and $b = 0$, and if $-b/c \neq 0$ then $c < 0$ and $a = 0$. The rest is clear. □

**Lemma 6.4** *The mapping $f(q_1) \mapsto f(q_2)$, $f \in \mathbb{Q}^+[x]$, is an isomorphism of the semiring A onto the semiring B.*

*Proof.* If $f_1(q_1) = f_2(q_1)$, then $\min_{\mathbb{Q}}(q_1)$ divides the difference $f_1 - f_2$. But then $(f_1 - f_2)(q_2) = 0$, and hence $f_1(q_2) = f_2(q_2)$. The rest is clear. $\square$

**Lemma 6.5** *Assume that $t \geq 0$. Then:*
(i) $A \subseteq \mathbb{Q}^+[\sqrt{q}]$.
(ii) *If $t = 0$, then $A = \mathbb{Q}^+[\sqrt{q}]$.*
(iii) *If $t \neq 0$, then $A \neq \mathbb{Q}^+[\sqrt{q}]$ and $A^* = \mathbb{Q}^+$.*

*Proof.* We have $q_1 \in \mathbb{Q}^+[\sqrt{q}]$ and the rest follows from 6.3. $\square$

**Lemma 6.6** *If $t \geq 0$, then $1 + t + \sqrt{q} \in A \setminus A^*$ and $1 + t - \sqrt{q} \in B \setminus B^*$.*

*Proof.* Use 6.5 and 6.4. $\square$

**Corollary 6.7** *If $t \geq 0$, then $0 \notin A$, $0 \notin B$, but neither $A$ nor $B$ is a parasemifield.*

**Lemma 6.8** (i) $\mathbb{Q}[\sqrt{q}]$ *is a subfield of* $\mathbb{R}$.
(ii) $\mathbb{Q}[\sqrt{q}]^+$ *is a subparasemifield of* $\mathbb{R}^+$.
(iii) *If $\sqrt{q} > -t$, then $A \subseteq \mathbb{Q}[q_1]^+ \subseteq \mathbb{Q}[\sqrt{q}]^+$.*

*Proof.* Easy to see. $\square$

**Lemma 6.9** *If $t \leq 0$, then $\sqrt{q} + \mathbb{Q}_0^+ \subseteq A$.*

*Proof.* We have $\sqrt{q} + a = (\sqrt{q} + t) + (a - t) = q_1 + a - t \in A$ for every $a \in \mathbb{Q}_0^+$. $\square$

**Lemma 6.10** *Let $a, b \in \mathbb{Q}$ be such that $a + b \in \mathbb{Q}^+$ and $-\sqrt{q} + a, -\sqrt{q} + b \in A$. Then $-\sqrt{q} + (q + ab)/(a + b) \in A$. Moreover, if $\sqrt{q} < a$ and $\sqrt{q} < b$, then $\sqrt{q} < (q + ab)/(a + b) < a, b$.*

*Proof.* We have $-\sqrt{q} + (q + ab)/(a + b) = (-\sqrt{q} + a)(-\sqrt{q} + b)/(a + b) \in A$. Moreover, if $\sqrt{q} < a$ and $\sqrt{q} < b$, then $ab + q - a\sqrt{q} - b\sqrt{q} = (a - \sqrt{q})(b - \sqrt{q}) > 0$, and so $\sqrt{q} < (q+ab)/(a+b)$. Finally, $q < a^2$, $q+ab < a^2+ab$ and $(q+ab)/(a+b) < a$. Similarly, $(q + ab)/(a + b) < b$. $\square$

**Lemma 6.11** *If $t < 0$, then $-\sqrt{q} + a \in A$ for every $a \in \mathbb{Q}^+$ such that $\sqrt{q} < a$.*

*Proof.* Put $t_1 = (q+t^2)/(-2t)$. We have $t_1 \in \mathbb{Q}^+$ and $-\sqrt{q}+t_1 = q_1^2/(-2t) \in A$. Since $q + t^2 + 2t\sqrt{q} = q_1^2 > 0$, we have $\sqrt{q} < t_1$. Now, by induction, put $t_{n+1} = (t_n^2 + q)/2t_n \in \mathbb{Q}^+$. According to 6.10, $t_1 > t_2 > t_3 > \cdots > \sqrt{q}$, and $-\sqrt{q} + t_n \in A$. If $t_0 = \lim t_n$, then $t_0 = (t_0^2 + q)/2t_0$, and hence $t_0 = \sqrt{q}$. Finally, if $\sqrt{q} < a$, $a \in \mathbb{Q}^+$, then $t_m < a$ for some $m \in \mathbb{N}$ and we have $a - t_m \in \mathbb{Q}^+$ and $-\sqrt{q} + a = (-\sqrt{q} + t_m) + (a - t_m) \in A$. $\square$

**Lemma 6.12** *Let $a, b \in \mathbb{Q}$ be such that $a + b \in \mathbb{Q}^+$ and $\sqrt{q} - a, -\sqrt{q} + b \in A$. Then $\sqrt{q} - (q + ab)/(a + b) \in A$. Moreover, if $0 < a < \sqrt{q} < b$, then $a < (q + ab)/(a + b) < \sqrt{q} < b$.*

*Proof.* We have $\sqrt{q} - (q + ab)/(a + b) = (\sqrt{q} - a)(-\sqrt{q} + b)/(a + b) \in A$. If $0 < a < \sqrt{q} < b$, then $a^2 < q$, $a^2 + ab < q + ab$ and $a < (q + ab)/(a + b)$. Moreover, $(\sqrt{q} - a)(b - \sqrt{q}) > 0$ and it follows that $q + ab < a\sqrt{q} + b\sqrt{q}$. $\square$

**Lemma 6.13** *If $t < 0$ and $\sqrt{q} > -t$, then $\sqrt{q} - a \in A$ for every $a \in \mathbb{Q}^+$ such that $\sqrt{q} > a$.*

*Proof.* Put $s_1 = (q - tt_1)/(t_1 - t)$, where $t_1 = (q + t^2)/(-2t)$, $\sqrt{q} < t_1$ (see the proof of 6.11). Since $0 < -t < \sqrt{q} < t_1$ and $\sqrt{q} - (-t), -\sqrt{q} + t_1 \in A$, we have, by 6.12, that $\sqrt{q} - s_1 \in A$ and $-t < s_1 < \sqrt{q}$. Now, by induction, put $s_{n+1} = (q + s_n t_1)/(s_n + t_1)$. According to 6.12, $s_1 < s_2 < s_3 < \cdots < \sqrt{q}$ and $\sqrt{q} - s_n \in A$. If $s_0 = \lim s_n$, then $s_0 = (q + s_0 t_1)/(s_0 + t_1)$, and hence $s_0 = \sqrt{q}$. Finally, if $a \in \mathbb{Q}^+$ is such that $\sqrt{q} > a$, then $a < s_m$ for some $m \in \mathbb{N}$ and we have $s_m - a \in \mathbb{Q}^+$ and $\sqrt{q} - a = = (\sqrt{q} - s_m) + (s_m - a) \in A$. □

**Lemma 6.14** *Let $0 < -t < \sqrt{q}$. Then:*
(i) *$a + \sqrt{q} \in A$ for every $a \in \mathbb{Q}_0^+$.*
(ii) *$b - \sqrt{q} \in A$ for every $b \in \mathbb{Q}^+$ with $\sqrt{q} < b$.*
(iii) *$-c + \sqrt{q} \in A$ for every $c \in \mathbb{Q}^+$ with $\sqrt{q} > c$.*

*Proof.* Combine 6.9, 6.11 and 6.13. □

**Lemma 6.15** *If $0 < -t < \sqrt{q}$, then $A = \mathbb{Q}[q_1]^+ = \mathbb{Q}[\sqrt{q}]^+$.*

*Proof.* Due to 6.8(iii), it is enough to show that $\mathbb{Q}[\sqrt{q}]^+ \subseteq A$. Hence, let $a, b \in \mathbb{Q}$ be such that $a + b\sqrt{q} > 0$. If $b = 0$, then $a \in \mathbb{Q}^+ \subseteq A$, so that we assume $b \neq 0$ and we put $c = a/|b|$. If $b > 0$, then $c + \sqrt{q} > 0$ and $c + \sqrt{q} \in A$ by 6.14(i),(iii); then $a + b\sqrt{q} \in A$, too. If $b < 0$, then $c - \sqrt{q} > 0$, $c \in \mathbb{Q}^+$, and $c - \sqrt{q} \in A$ by 6.14(ii); then $a + b\sqrt{q} \in A$, too. □

**Proposition 6.16** (i) *If $\sqrt{q} < -t$, then $A = \mathbb{Q}[\sqrt{q}]$ and $A^* = \mathbb{Q}[\sqrt{q}] \setminus \{0\}$.*
(ii) *If $t = 0$, then $A = \mathbb{Q}^+[\sqrt{q}] \subsetneqq \mathbb{Q}[\sqrt{q}]^+$ and $A^* = \{a, a\sqrt{q} \mid a \in \mathbb{Q}^+\}$.*
(iii) *If $t > 0$, then $A \subsetneqq \mathbb{Q}^+[\sqrt{q}]$ and $A^* = \mathbb{Q}^+$.*
(iv) *If $0 < -t < \sqrt{q}$, then $A = A^* = \mathbb{Q}[q_1]^+ = \mathbb{Q}[\sqrt{q}]^+$.*

*Proof.* (i) Put $C = A \cap \mathbb{Q}$. Then $\mathbb{Q}^+ \subseteq C$ and $q - t^2 = (\sqrt{q} + t)(\sqrt{q} - t) = q_1(q_1 - 2t) \in \in C \cap \mathbb{Q}^-$. Now, $C$ is a subsemiring of $\mathbb{Q}$ containing all positive rational numbers and at least one negative rational number. Then $C = \mathbb{Q}$, $\mathbb{Q} \subseteq A$, $\sqrt{q} \in A$ and, finally, $A = \mathbb{Q}[\sqrt{q}]$.

(ii) Clearly, if $0 < r < \sqrt{q}$, $r \in \mathbb{Q}^+$, then $\sqrt{q} - r \in \mathbb{Q}[\sqrt{q}]^+$ and $\sqrt{q} - r \notin \mathbb{Q}^+[\sqrt{q}]$. The rest follows from 6.3(ii).

(iii) See 6.5(iii).

(iv) See 6.15. □

**Proposition 6.17** (i) *If $\sqrt{q} < -t$, then $B = \mathbb{Q}[\sqrt{q}]$ and $B^* = \mathbb{Q}[\sqrt{q}] \setminus \{0\}$.*
(ii) *If $t = 0$, then $B = \mathbb{Q}^+[-\sqrt{q}]$ and $B^* = \{a, -a\sqrt{q} \mid a \in \mathbb{Q}^+\}$.*
(iii) *If $t > 0$, then $B \subsetneqq \{a - b\sqrt{q} \mid a, b \in \mathbb{Q}_0^+, a + b \neq 0\}$ and $B^* = \mathbb{Q}^+$.*
(iv) *If $0 < -t < \sqrt{q}$, then $B = B^* = \{a - b\sqrt{q} \mid a, b \in \mathbb{Q}, a > -b\sqrt{q}\}$.*

*Proof.* The map $\varphi : \mathbb{Q}[q_1] \to \mathbb{Q}[q_2]$, $\varphi(f(q_1)) = f(q_2)$, $f \in \mathbb{Q}[x]$, is an isomorphism of fields. Let $a, b \in \mathbb{Q}$. We have $\varphi(a + b\sqrt{q}) = \varphi((a - bt) + bq_1) = (a - bt) + bq_2 = = a - b\sqrt{q}$.

(i) Let $\sqrt{q} < -t$. Then, by 6.14, $A = \mathbb{Q}[\sqrt{q}]$. Hence $B = \varphi(A) = \varphi(\mathbb{Q}[\sqrt{q}]) = \mathbb{Q}[\sqrt{q}]$.

(ii) Use 6.4 and 6.16.

(iii),(iv) Similar to (i). □

**Corollary 6.18** *(cf. 6.2) The following conditions are equivalent:*

(i) $\sqrt{q} > -t > 0$.

(ii) *$A$ is a parasemifield.*

(iii) *$B$ is a parasemifield.*

*Proof.* Use 6.17. □

**Corollary 6.19** *The following conditions are equivalent:*

(i) $\sqrt{q} < -t$.

(ii) *$A$ ($B$, resp.) is a field.*

(iii) *$A$ ($B$, resp.) is a semifield.*

(iv) *$0 \in A$ ($0 \in B$, resp.).*

## 7. The subsemirings $\mathbb{Q}^+[\alpha], \alpha \in \mathbb{C}$

**Proposition 7.1** *Let $\alpha \in \mathbb{C}$ be algebraic of degree 2. The following conditions are equivalent:*

(i) $0 \notin \mathbb{Q}^+[\alpha]$.

(ii) $a_0 + a_1\alpha + \cdots + a_n\alpha^n \neq 0$ *whenever* $n \in \mathbb{N}_0$, $a_i \in \mathbb{Q}_0^+$ *and* $\sum a_i \neq 0$.

(iii) *There exist $q \in \mathbb{Q}^+$ and $t \in \mathbb{Q}$ such that $\sqrt{q} \notin \mathbb{Q}$, $\sqrt{q} > -t$ and either $\alpha = t + \sqrt{q}$ or $\alpha = t - \sqrt{q}$.*

*Proof.* Clearly, (i) is equivalent to (ii).

(ii) implies (iii). Put $f = \min_{\mathbb{Q}}(\alpha)$, $\deg(f) = 2$. It follows from (ii) and 5.4 that $f$ has a positive real root and it remains to apply 5.8.

(iii) implies (i). See 6.2. □

**Proposition 7.2** *Let $\alpha \in \mathbb{C}$ be algebraic of degree 2. Then $\mathbb{Q}^+[\alpha]$ is a parasemifield if and only if there exist $q \in \mathbb{Q}^+$ and $t \in \mathbb{Q}^-$ such that $\sqrt{q} \notin \mathbb{Q}$, $\sqrt{q} > -t$ and either $\alpha = t + \sqrt{q}$ or $\alpha = t - \sqrt{q}$. Moreover, if $\alpha = t + \sqrt{q}$, then $\mathbb{Q}^+[\alpha] = \mathbb{Q}[\sqrt{q}]^+$ and, if $\alpha = t - \sqrt{q}$, then $\mathbb{Q}^+[\alpha] = \{a - b\sqrt{q} \mid a, b \in \mathbb{Q}, a > -b\sqrt{q}\}$.*

*Proof.* Combine 7.1, 6.16(ii),(iii),(iv) and 6.17(ii),(iii),(iv). □

**Lemma 7.3** *Let $\alpha \in \mathbb{C}$ be an algebraic number such that $\mathbb{Q}^+[\alpha] \cap \mathbb{Q}^- \neq \emptyset$. Then $\mathbb{Q}^+[\alpha] = \mathbb{Q}[\alpha]$ (a subfield of $\mathbb{C}$).*

*Proof.* Put $A = \mathbb{Q}^+[\alpha] \cap \mathbb{Q}$. Then $A$ is a subsemiring of $\mathbb{Q}$, $\mathbb{Q}^+ \subseteq A$ and $A \cap \mathbb{Q}^- \neq \emptyset$. Consequently, $A = \mathbb{Q}$ and $\mathbb{Q}^+[\alpha] = \mathbb{Q}[\alpha]$. □

**Proposition 7.4** *Let $\alpha \in \mathbb{C}$ be an algebraic number. The following conditions are equivalent:*

(i) $0 \notin \mathbb{Q}^+[\alpha]$.
(ii) $a_0 + a_1\alpha + \cdots + a_n\alpha^n \neq 0$ *whenever* $n \in \mathbb{N}_0$, $a_i \in \mathbb{Q}_0^+$ *and* $\sum a_i \neq 0$.
(iii) *The minimal polynomial* $\min_{\mathbb{Q}}(\alpha)$ *has a positive real root.*

*Proof.* See 5.5. □

**Proposition 7.5** *Let $\alpha \in \mathbb{C}$, $\alpha \neq 0$, be an algebraic number. The following conditions are equivalent:*
(i) $\mathbb{Q}^+[\alpha] = \mathbb{Q}[\alpha]$ *(a subfield of $\mathbb{C}$).*
(ii) $0 \in \mathbb{Q}^+[\alpha]$.
(iii) *The minimal polynomial* $\min_{\mathbb{Q}}(\alpha)$ *has no positive real roots.*

*Proof.* First, (ii) is equivalent to (iii) by 7.4 and (i) implies (ii) trivially. It remains to show that (ii) implies (i). If $0 \in \mathbb{Q}^+[\alpha]$, then there are $n \in \mathbb{N}$ and $a_0, \dots, a_n \in \mathbb{Q}_0^+$ such that $0 = a_0 + a_1\alpha + \cdots + a_n\alpha^n$ and $a_n \neq 0$. Assume that $n$ is the smallest possible. Then $a_0 > 0$ and $-a_0 = a_1\alpha + \cdots + a_n\alpha^n \in \mathbb{Q}^+[\alpha] \cap \mathbb{Q}^-$. By 7.3, $\mathbb{Q}^+[\alpha] = \mathbb{Q}[\alpha]$. □

**Proposition 7.6** *Let $\alpha \in \mathbb{C}$ be an algebraic number such that $\beta^m = 1$ for some $\beta \in \mathbb{Q}^+[\alpha]$, $\beta \neq 1$, and $m \geq 2$. Then $\mathbb{Q}^+[\alpha] = \mathbb{Q}[\alpha]$.*

*Proof.* We have $\beta\gamma = \gamma$, where $\gamma = 1 + \beta + \cdots + \beta^{m-1} \in \mathbb{Q}^+[\alpha]$. Since $\beta \neq 1$, it follows that $\gamma = 0$, and hence $0 \in \mathbb{Q}^+[\alpha]$. It remains to use 7.5. □

**Remark 7.7** (i) If $\alpha \in \mathbb{C}$ is transcendental, then $A = \mathbb{Q}^+[\alpha] \cong \mathbb{Q}^+[x]$. In particular, $0 \notin A$ and $AA^{-1} = \{ab^{-1} | \, a, b \in A\}$ is a subparasemifield of $\mathbb{C}$. Clearly, $AA^{-1}$ is a free parasemifield freely generated by $\{\alpha\}$.

(ii) If $\alpha \in \mathbb{C}$ is algebraic number satisfying the equivalent conditions of 7.4, then $0 \notin A$ and $AA^{-1} = \{ab^{-1} | \, a, b \in A\}$ is a subparasemifield of $\mathbb{C}$.

**Proposition 7.8** *Let $\alpha \in \mathbb{C}$ and $A = \mathbb{Q}^+[\alpha]$. The following conditions are equivalent:*
(i) *$A$ is contained in a subparasemifield of $\mathbb{C}$.*
(ii) $0 \notin A$.
(iii) *Either $\alpha$ is transcendental or $\alpha$ is algebraic and the minimal polynomial* $\min_{\mathbb{Q}}(\alpha)$ *has a positive real root.*

*Proof.* Combine 7.4 and 7.7. □

## 8. Free parasemifields

Let $X$ be a set and $\mathbf{P}(X) = \{f/g | \, f, g \in \mathbb{N}_0[X], f \neq 0 \neq g\}$. Then $\mathbf{P}(X)$ is a free parasemifield over $X$. (Notice that $\mathbf{P}(\emptyset) = \mathbb{Q}^+$.)

In the remaining part of this section, assume that $X = \{x\}$ is a one-element set and put $\mathbf{P} = \mathbf{P}(x)$. That is, $\mathbf{P}$ is a free parasemifield of rank 1.

For every $f \in \mathbb{N}_0[x]$, $f \neq 0$, there exist uniquely determined $\mathrm{v}(f) \in \mathbb{N}_0$ and $f_1 \in \mathbb{N}_0[x]$ such that $f = x^{\mathrm{v}(f)} \cdot f_1$ and $x$ doesn't divide $f_1$. If $f, g \in \mathbb{N}_0[x] \setminus \{0\}$, then $\mathrm{v}(fg) = \mathrm{v}(f) + \mathrm{v}(g)$. Consequently, for $f/g \in \mathbf{P}$, we can put $\mathrm{v}(f/g) = \mathrm{v}(f) - \mathrm{v}(g) \in \mathbb{Z}$.

**Lemma 8.1** $\mathrm{v}(FG) = \mathrm{v}(F)+\mathrm{v}(G)$ *and* $\mathrm{v}(F+G) = \min(\mathrm{v}(F), \mathrm{v}(G))$ *for all* $F, G \in \mathbf{P}$.

*Proof.* Let $F = x^n f_1/g_1$ and $G = x^m f_2/g_2$, where $x$ doesn't divide $f_i, g_i$ for $i = 1, 2$. We can consider $n \geq m$. Then $x^n f_1/g_1 + x^m f_2/g_2 = x^m(x^{n-m} f_1 g_2 + f_2 g_1)/g_1 g_2$. Since $x$ doesn't divide $x^{n-m} f_1 g_2 + f_2 g_1$, we have $\mathrm{v}(F + G) = m = \min(\mathrm{v}(F), \mathrm{v}(G))$. The rest is obvious. □

**Remark 8.2** Define a relation $\xi$ on $\mathbf{P}$ by $(F, G) \in \xi$ iff $\mathrm{v}(F) = \mathrm{v}(G)$. It follows easily from 8.1 that $\xi$ is a congruence of the parasemifield $\mathbf{P}$. Since $(1, 2) \in \xi$, the factor $\mathbf{P}/\xi$ is an additively idempotent parasemifield. In fact, $\varphi : \mathbf{P} \to \mathbb{Z}(\oplus, +)$, $\varphi(F/\xi) = \mathrm{v}(F)$ is an isomorphism of parasemifields where $m \oplus n = \min(n, m)$.

**Remark 8.3** Let $\alpha \in \mathfrak{A}$ (see 5.5). The mapping $\kappa_\alpha : \mathbf{P} \to \mathbb{C}$, $f/g \mapsto f(\alpha)/g(\alpha)$, is a homomorphism and $\kappa_\alpha(\mathbf{P})$ is a subparasemifield of $\mathbb{C}$ (see 7.7). The equivalence $\ker(\kappa_\alpha)$ is a congruence of $\mathbf{P}$.

**Remark 8.4** Consider the parasemifield $\mathbb{Q}^+ \times \mathbb{Z}(\oplus, +)$ (see 8.2). Then $(1, 0)$, is unit element and we have $(1, 1) + (1, 0) = (2, 0) = (1, 0) + (1, 0)$ (cf. [2, 4.13])

**Remark 8.5** Put $\tau = \xi \cap \ker(\kappa_\alpha)$, where $\alpha = 1 \in \mathbb{Q}^+$ (see 8.2 and 8.3). Then $\tau$ is a congruence of the parasemifield $\mathbf{P}$. It is easy to see that $\psi : \mathbf{P}/\tau \to \mathbb{Q}^+ \times \mathbb{Z}(\oplus, +)$, $\psi(F/\tau) = (F(1), \mathrm{v}(F))$ is an isomorphism of parasemifields (see 8.4).

**Remark 8.6** Define an operation $\boxplus$ on $\mathbb{Q}^+ \times \mathbb{Z}$ by $(r, m) \boxplus (s, n) = (r, m)$ if $m < n$, $(r, m) \boxplus (s, n) = (r + s, m)$ if $m = n$ and $(r, m) \boxplus (s, n) = (s, n)$ if $n < m$. One checks easily that $P = (\mathbb{Q}^+ \times \mathbb{Z})(\boxplus, *)$ is parasemifield, where $(r, m) * (s, n) = (rs, m + n)$ (cf. 8.4). Notice that $(r, m) \boxplus (r, m) = (2r, m) \neq (r, m)$ and $\rho_P = P \times P$ (see [2, 1.10]) (cf. [2, 1.12(ii)]).

**Remark 8.7** Define a relation $\chi$ on $\mathbf{P}$ by $(F, G) \in \chi$ iff $\mathrm{v}(F) = \mathrm{v}(G)$ (i.e., $(F, G) \in \in \xi$) and $(x^{-\mathrm{v}(F)}F)(0) = (x^{-\mathrm{v}(G)}G)(0)$. It follows easily from 8.1 that $\chi$ is a congruence of $\mathbf{P}$. Moreover, $\pi : \mathbf{P}/\chi \to (\mathbb{Q}^+ \times \mathbb{Z})(\boxplus, *)$, $\pi(F/\chi) = ((x^{-\mathrm{v}(F)}F)(0), \mathrm{v}(F))$ is an isomorphism of parasemifields (see 8.6).

## 9. Free additively idempotent parasemifields

Define operations $\oplus$ and $\odot$ on $\{0, 1\}$ ($\subseteq \mathbb{N}$) by $u \oplus v = \max\{u, v\}$ and $u \odot v = \min\{u, v\}$ for $u, v \in \{0, 1\}$. It is easy to see that $S = (\{0, 1\}, \oplus, \odot)$ is an additively idempotent semiring. Let $X$ be a set and $\mathbf{S}[X]$ a semiring of non-zero polynomials over $S$ and $X$.

For $(a, b), (c, d) \in \mathbf{S}[X] \times \mathbf{S}[X]$ put $(a, b) + (c, d) = (ad + bc, bd)$ and $(a, b) \cdot (c, d) = = (ac, bd)$. Define relation $\equiv$ on $\mathbf{S}[X] \times \mathbf{S}[X]$ as follows: $(a, b) \equiv (c, d)$ iff there is $e \in \mathbf{S}[X]$ such that $ade = bce$.

**Remark 9.1** $\mathbf{S}[X]$ is a free unitary additively idempotent semiring with basis $X$. Further, it is easy to verify that $\mathbf{S}[X] \times \mathbf{S}[X]$ is a semiring and $\equiv$ a congruence on $\mathbf{S}[X] \times \mathbf{S}[X]$.

Put $\mathbf{G}(X) = \mathbf{S}[X] \times \mathbf{S}[X]/\equiv$ and denote $a/b$ the congruence class of $\equiv$ containg $(a, b) \in \mathbf{S}[X] \times \mathbf{S}[X]$.

**Remark 9.2** Obviously, $\mathbf{G}(X)$ is an additively idempotent parasemifield.

**Lemma 9.3** *$\mathbf{G}(X)$ is a free additively idempotent parasemifield with basis* $\overline{X} = \{x/1 | x \in X\}$.

*Proof.* Clearly, $x/1 \neq x'/1$ for $x, x' \in X$, $x \neq x'$ and $\mathbf{G}(X)$ is generated by $\overline{X}$.

Let $P$ be an additively idempotent parasemifield and $\psi : \overline{X} \to P$ a map. By 9.1, there is a homomorphism $\varphi : \mathbf{S}[X] \to P$ such that $\varphi(x) = \psi(x/1)$ for every $x \in X$.

Let be now $a/b = c/d \in \mathbf{G}(X)$. Then there is $e \in \mathbf{S}[X]$ such that $ade = bce$, hence $\varphi(a)\varphi(d)\varphi(e) = \varphi(b)\varphi(c)\varphi(e)$ and $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$, since $P$ is a parasemifield. Now, $\Phi : \mathbf{G}(X) \to P$, $\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$ for $a/b \in \mathbf{G}(X)$ is a (well defined) homomorphism such that $\Phi(x/1) = \psi(x/1)$ for every $x/1 \in \overline{X}$. $\square$

**Remark 9.4** $\mathbf{S}[X]$ is not multiplicatively cancellative; e.g., $(1 + x)(1 + x^2) = 1 + x + x^2 + x^3 = (1 + x)(1 + x + x^2)$, thus $(1 + x^2)/1 = (1 + x + x^2)/1$ in $\mathbf{G}(X)$, but $1 + x^2 \neq 1 + x + x^2$ in $\mathbf{S}[X]$.

## References


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

[2] Kala, V., Kepka, T., Korbelář, M.: *Notes on commutative parasemifields* (preprint).