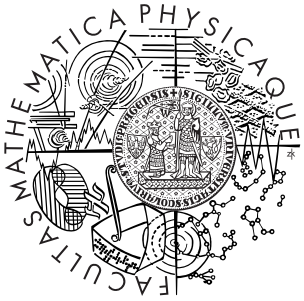
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Vítězslav Kala

Jednoduché poolookruhy

Katedra algebry

Vedoucí bakalářské práce: Prof. RNDr. Tomáš Kepka, DrSc.

Studijní program: Obecná matematika, Matematické struktury

2007

Děkuji Sašovi Kazdovi za jeho nedocenitelnou pomoc při mém zápolení s LaTeXem.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 30. května 2007 Vítězslav Kala

Contents

1 Introduction **5**

2 Some known facts about semirings **6**

3 p-divisible semirings **9**

4 Full congruence-simple semirings **11**

Bibliography **18**

Název práce: Jednoduché polookruhy
Autor: Vítězslav Kala
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Prof. RNDr. Tomáš Kepka, DrSc.
e-mail vedoucího: kepka@karlin.mff.cuni.cz

Abstrakt: Kongruenčně jednoduché polookruhy jsou už charakterizované s výjimkou podpolookruhů $\mathbb{R}^+$. Dokonce ani podpolookruhy $\mathbb{Q}^+$ dosud nejsou popsané. V práci dokazujeme tvrzení, že každý kongruenčně jednoduchý polookruh $S \subseteq \mathbb{Q}^+$ je p-dělitelný pro nějaké prvočíslo p (tedy že $\mathbf{v}_p(q) > 0$ pro každé $q \in S \cap (0,1)$). Pomocí něj potom klasifikujeme polookruhy $S \subseteq \mathbb{Q}^+$ takové, že pro $x \in \mathbb{Q}^+ \backslash \{1\}$ platí $x \in S$ právě tehdy, když $1/x \notin S$ (takzvané plné polookruhy).
Klíčová slova: polookruh, komutativní, jednoduchý, plný

Title: Simple Semirings
Author: Vítězslav Kala
Department: Department of Algebra
Supervisor: Prof. RNDr. Tomáš Kepka, DrSc.
Supervisor's e-mail address: kepka@karlin.mff.cuni.cz

Abstract: Congruence-simple semirings have already been characterized with the exception of the subsemirings of $\mathbb{R}^+$. Even the subsemirings of $\mathbb{Q}^+$ have not been classified yet. In the work we prove the fact that every congruence-simple semiring $S \subseteq \mathbb{Q}^+$ is p-divisible for a prime p (i.e., $\mathbf{v}_p(q) > 0$ for all $q \in S \cap (0,1)$). This we use for the characterization of congruence-simple semirings $S \subseteq \mathbb{Q}^+$ such that if $x \in \mathbb{Q}^+ \backslash \{1\}$ then $x \in S$ if and only if $1/x \notin S$ (the so called full semirings).
Keywords: semiring, commutative, simple, full

Chapter 1

Introduction

Congruence-simple semirings are characterized in [1] (see 2.9). Only the subsemirings of $\mathbb{R}^+$ have not yet been classified up to isomorphism. Even the subsemirings of $\mathbb{Q}^+$ have not been classified yet. The aim of this work is to begin the classification of the subsemirings of $\mathbb{Q}^+$.

In the third chapter we prove that every such semiring is p-divisible for a prime p (i.e., $\mathbf{v}_p(q) > 0$ for all $q \in S \cap (0,1)$), which is a useful property for the classification.

In the fourth chapter we characterize the full congruence-simple semirings (i.e., such semirings that if $x \in \mathbb{Q}^+ \backslash \{1\}$ then $x \in S$ if and only if $1/x \notin S$). These semirings seem to be a good starting point for the general classification - every full subsemiring $S \subseteq \mathbb{Q}^+$ is a maximal one (i.e., if $S \subseteq T \subseteq \mathbb{Q}^+$ and T is a congruence-simple semiring, then $T = S$ or $T = \mathbb{Q}^+$) and it seems that there are almost no other maximal subsemirings of $\mathbb{Q}^+$. The methods used for the characterization can be to some extent used also in the general case, unfortunately we have not even succeeded in characterizing the maximal semirings yet.

Many examples of congruence-simple subsemirings of $\mathbb{Q}^+$ can be obtained as intersections of the (defined) semirings $\mathbb{T}_p(x)$, in fact every known (at least to the author) example of a congruence-simple subsemiring of $\mathbb{Q}^+$ is of this form. Each of the semirings $\mathbb{T}_p(x)$ is maximal.

Chapter 2

Some known facts about semirings

2.1 Definition A semiring S is a non-empty set with two binary operations - addition $(+)$ and multiplication $(\cdot)$ such that

i) both operations are associative, i.e. $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in S$,

ii) the addition is commutative, i.e. $a + b = b + a$ for all a, b,

iii) the multiplication is distributive over the addition, i.e. $(a + b) \cdot c = a \cdot c + b \cdot c$ and $c \cdot (a + b) = c \cdot a + c \cdot b$ for all $a, b, c \in S$.

A semiring is commutative if moreover

iv) the multiplication is commutative, i.e. $a \cdot b = b \cdot a$ for all $a, b \in S$.

We will be dealing only with commutative semirings, and so "semiring" will always mean a commutative semiring.

2.2 Definition Let S be a semiring. The semiring is said to be

a) additively idempotent if $a + a = a$ for each $a \in S$,

b) multiplicatively idempotent if $a \cdot a = a$ for each $a \in S$,

c) additively cancellative if for all $a, b, c \in S$ $a + b = a + c$ implies $b = c$.

d) multiplicatively cancellative if for all $a, b, c \in S$ $a \cdot b = a \cdot c$ implies $b = c$.

2.3 Definition Let S be a semiring. A (binary) relation $r \subseteq S \times S$ is a congruence of S if

i) r is an equivalence (i.e. r is reflexive ($(a,a) \in r$), symmetric (if $(a,b) \in r$ then $(b,a) \in r$), and transitive (if $(a,b),(b,c) \in r$ then $(a,c) \in r$)),

ii) if $(a,b) \in r$ and $c \in S$ then $(a+c, b+c) \in r$ and $(ac, bc) \in r$.

2.4 Definition Let S be a semiring. A non-empty subset I of S is an ideal of S if $SI \subseteq I$ and $I + I \subseteq I$. A non-empty subset I of S is a bi-ideal of S if $SI \subseteq I$ and $S + I \subseteq I$.

2.5 Definition Let S be a semiring. The semiring is said to be

a) congruence-simple if S is non-trivial and id_S, $S \times S$ are the only congruences of S,

b) ideal-simple if S is non-trivial and $I = S$ for every ideal of S containing at least two elements.

c) bi-ideal-simple if S is non-trivial and $I = S$ for every bi-ideal of S containing at least two elements.

2.6 Theorem [1, 8.2] *Let S be a non-trivial semiring that is additively and multiplicatively cancellative. Then S is congruence-simple if and only if S satisfies the following three conditions:*

i) For all $a, b \in S$ there exists $c \in S$ and $n \in \mathbb{N}$ such that $b + c = na$ (i.e., S is archimedian).

ii) 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).

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

2.7 [1, 3.2] Let $G(\cdot)$ be an abelian group, $o \notin G$. Put $V(G) = G \cup \{o\}$ and define $x+y = y+x = o, x+x = x$ and $xo = ox = o$ for all $x, y \in V(G), x \neq y$. $V(G)$ is clearly an additively idempotent semiring.

2.8 [1, 5.1] Let A be a non-zero subsemigroup of $\mathbb{R}(+)$. Denote $W(A) = W(\oplus, *)$ the following (additively idempotent and multiplicatively cancellative) semiring: $W(A) = A$, $a \oplus b = b \oplus a = \min(a, b)$ and $a * b = b * a = a + b$ for all $a, b \in A$.

2.9 Theorem [1, 10.1] *A semiring S, $|S| \geq 3$, is congruence-simple if and only if S is isomorphic to one of the following semirings:*

(1) *the semirings $V(G)$ for an abelian group G,*

(2) *the semirings $W(A)$ for a subsemigroup A of $\mathbb{R}(+)$ such that $A \cap \mathbb{R}^+ \neq \emptyset \neq A \cap \mathbb{R}^-$,*

(3) *fields,*

(4) *zero-multiplication rings of finite prime order,*

(5) *the subsemirings S of $\mathbb{R}^+$ satisfying the conditions of* 2.6.

2.10 Lemma [1, 9.1] *A subsemiring S of $\mathbb{Q}^+$ is archimedian and conical if and only if for every $n \in \mathbb{N}$ there exists $m \in \mathbb{N}$ such that $\frac{k}{n} \in S$ for every $k \geq m$.*

2.11 Lemma [1, 9.4] *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 $1/s \in S$ where s is the least common multiple of b and d and S is the subsemiring of $\mathbb{Q}^+$ generated by $\frac{a}{b}, \frac{c}{d}$.*

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

Chapter 3

p-divisible semirings

3.1 Definition Let p be a prime number, $q \in \mathbb{Q} \setminus \{0\}$. Let $n \in \mathbb{N}$ be such that $q = p^n \frac{r}{s}$, where $r \in \mathbb{Z}, s \in \mathbb{N}$, $p \nmid r$, $p \nmid s$. We define the p-valuation of q as $\mathbf{v}_p(q) = n$.

For $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (p_i are pairwise different primes) define that n divides q ($n \mid q$) if $\mathbf{v}_{p_i}(q) \geq \alpha_i$ for all i and that n does not divide q ($n \nmid q$) otherwise.

3.2 Lemma. *Let p be a prime number and $q_1, \ldots, q_n \in \mathbb{Q} \setminus \{0\}$. If $\mathbf{v}_p(q_i)$ are pairwise different then $\mathbf{v}_p(q_1 + \ldots + q_n) = \min\{\mathbf{v}_p(q_i)\}$.*

Proof. For $i \in \{1, 2, \ldots, n\}$ denote $k_i = \mathbf{v}_p(q_i)$ and let $q_i = p^{k_i} \frac{r_i}{s_i}$, where $r_i \in \mathbb{Z}, s_i \in \mathbb{N}$, $p \nmid r_i$, $p \nmid s_i$. Let $k = \min\{k_i\} = k_j$.

Then $q_1 + q_2 + \ldots + q_n = p^k \sum_{i=1}^{n} p^{k_i - k} \frac{r_i}{s_i} = p^k (\frac{r_j}{s_j} + p \sum_{i \neq j} p^{k_i - k - 1} \frac{r_i}{s_i})$, and so $\mathbf{v}_p(q_1 + \ldots + q_n) = k$. □

3.3 Lemma *Let $p_1, \ldots, p_k$ be prime numbers and $a_1, \ldots a_k \in \mathbb{Q} \cap (0, 1)$ such that $p_i \nmid a_i$ for $i = 1, \ldots k$, $k \in \mathbb{N}$. Let S be a semiring generated by $a_1, \ldots a_k$. Then there exists $b \in S \cap (0, 1)$ such that $p_i \nmid b$ for all $i = 1, \ldots, k$.*

Proof. Let $n \in \mathbb{N}$ be such that $n > k$ and $a_i^n < \frac{1}{k \cdot (p_1 \cdot \ldots \cdot p_k)^k}$ for all $i = 1, \ldots, k$. Put $b_i = a_i^n (p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_k)^i \in S$. Now, $b_i < a_i^n (p_1 \ldots p_k)^i \leq a_i^n (p_1 \ldots p_k)^k < \frac{1}{k}$, $b = b_1 + \ldots + b_k < 1$ and $b \in S \cap (0, 1)$.

$\mathbf{v}_{p_i}(b_j) = n \cdot \mathbf{v}_{p_i}(a_j) + j$ for $j \neq i$ and $\mathbf{v}_{p_i}(b_i) = n \cdot \mathbf{v}_{p_i}(a_i)$ for all $i = 1, \ldots, k$. For $l \neq m$ clearly $\mathbf{v}_{p_i}(b_l) \neq \mathbf{v}_{p_i}(b_m)$, and so from 3.2 follows that $\mathbf{v}_{p_i}(b) = \min\{\mathbf{v}_{p_i}(b_j)\} \leq \mathbf{v}_{p_i}(b_i) = n \cdot \mathbf{v}_{p_i}(a_i) \leq 0$. □

3.4 Lemma *Let $S \subseteq \mathbb{Q}^+$ be a semiring. If for all $\frac{k}{l}, \frac{m}{n} \in S \cap (0,1)$ ($\gcd(k,l) = \gcd(m,n) = 1$) is $\gcd(k,m) > 1$ then there exists a prime p such that $p \mid a$ for all $a \in S \cap (0,1)$.*

Proof. Let $x \in S \cap (0,1)$, $x = \frac{k}{l}$ ($\gcd(k,l) = 1$) and let $k = p_1^{a_1} \ldots p_n^{a_n}$ where p_i are pairwise different primes. Assume for contradiction that for every $i = 1, \ldots, n$ there exists $x_i \in S \cap (0,1)$ such that $p_i \nmid x_i$. From 3.3 follows the existence of $t \in S \cap (0,1)$ such that $p_i \nmid t$ for all $i = 1, \ldots, n$. But $t = \frac{x}{y}$, $\gcd(x,y) = 1$, $p_i \nmid x$ for $i = 1, \ldots, n$, which is a contradiction with $\gcd(x,k) > 1$. □

3.5 Lemma *Let $S \subseteq \mathbb{Q}^+$ be a semiring, $1 \notin S$. Then there exists a prime p such that $p \mid a$ for all $a \in S \cap (0,1)$.*

Proof. Let $\frac{k}{l}, \frac{m}{n} \in S \cap (0,1)$, $\gcd(k,l) = 1 = \gcd(m,n)$. If $\gcd(k,m) = 1$ then by 2.11 $\frac{1}{s} \in S$ and also $s \cdot \frac{1}{s} = 1 \in S$, where s is the least common multiple of l and n. Thus $\gcd(k,m) > 1$ and the statement follows from 3.4. □

3.6 Definition Let $S \subseteq \mathbb{Q}^+$ be a semiring. If there exists $d \in \mathbb{N} \setminus \{1\}$ such that $d \mid a$ for all $a \in S \cap (0,1)$ then we call S d-divisible semiring.

3.7 Theorem *Let $S \subsetneq \mathbb{Q}^+$ be a congruence-simple semiring. Then there exists a prime p such that S is p-divisible.*

Proof. If $1 \in S$ then by 2.12 $S = \mathbb{Q}^+$. So $1 \notin S$ and we can use 3.5. □

3.8 Lemma *a) Let p be a prime and $i \in \mathbb{Z}$. Then $\{q \mid q \in \mathbb{Q}, \mathbf{v}_p(q) = i\}$ is a dense set.*

b) Let p, q be primes and $i, j \in \mathbb{Z}$. Then $\{q \mid q \in \mathbb{Q}, \mathbf{v}_p(q) = i, \mathbf{v}_p(q) = j\}$ is a dense set.

Proof. Easy. □

Chapter 4

Full congruence-simple semirings

4.1 Definition Let $S \subseteq \mathbb{Q}^+$ be a semiring. If $x \in S \Leftrightarrow \frac{1}{x} \notin S$ for all $x \in \mathbb{Q}^+ \setminus \{1\}$ then S is said to be full.

4.2 Let $S \subseteq \mathbb{Q}^+$ be a congruence-simple semiring. It follows from 2.6 and 2.10 that for all $n \in \mathbb{N}$ there exists $m \in \mathbb{N}$ such that $\frac{k}{n} \in S$ for all $k \geq m$. Let m be the minimal number satisfying this condition, denote $\mathbf{a}_S(n) = \frac{m-1}{n}$. Then $\mathbf{a}_S(n)$ is the least number satisfying:
1) $n \cdot \mathbf{a}_S(n) \in \mathbb{N}$.
2) If $\frac{k}{n} > \mathbf{a}_S(n)$ then $\frac{k}{n} \in S$.

4.2.1 Lemma *If S is full then $1 \notin S$.*

Proof. By 2.12 if $1 \in S$ then $S = \mathbb{Q}^+$ and also $\frac{1}{2}, 2 \in S$. □

4.2.2 Lemma *If S is full then $\mathbf{a}_S(n) \geq 1$ for all $n \in \mathbb{N}$.*

Proof. Easy, because $\frac{n}{n} \notin S$. □

4.2.3 Lemma *Let $d \in \mathbb{N} \setminus \{1\}$ and $k \in \mathbb{N}$. If $d \nmid k$ and S is full and d-divisible, then $\mathbf{a}_S(k) = 1$.*

Proof. If $\mathbf{a}_S(k) > 1$ then $\frac{k+1}{k} \notin S$, and so $\frac{k}{k+1} \in S$, a contradiction with the assumption that S is d-divisible. $\square$

4.3 Let S be full p-divisible semiring for a prime p; denote $T = S \cap (0,1)$. Then by 2.6 is S bi-ideal-simple and for all $a, b \in S$ there exist $c, d \in S$ such that $a = bc + d$. If $a < b$ then $c \in T$.

Now, let $\mathbf{V}_p(S) = \min\{\mathbf{v}_p(x), x \in T\}$ ($\mathbf{V}_p(S)$ exists because $T \neq \emptyset$ and $\mathbf{v}_p(x) > 0$ for all $x \in T$).

Furthemore, let's define $B_{pr} = \{\frac{pr}{s} \in T \mid s \in \mathbb{N} \text{ and } p \nmid s\}$ for all $r \in \mathbb{N}$. If $\frac{s}{pr} > \mathbf{a}_S(pr)$ then $\frac{s}{pr} \in S$ and $\frac{pr}{s} \notin S$, and so B_{pr} is finite for all $r \in \mathbb{N}$.

$R = \{pr \mid B_{pr} \neq \emptyset\}$ is non-empty; let $\beta(pr) = \min B_{pr}$ for $pr \in R$. For $i \geq \mathbf{V}_p(S)$ put $R_i = \{p^i r \mid B_{p^i r} \neq \emptyset, p \nmid r\}$.

4.3.1 Lemma *$R_i \neq \emptyset$ for $i \geq \mathbf{V}_p(S)$.*

Proof. For $i = \mathbf{V}_p(S)$ is $R_i \neq \emptyset$ by definition (see 3.5) and there exists $\frac{p^{\mathbf{V}_p(S)} r}{s} \in R_i$, $p \nmid r$ and $p \nmid s$.

Let $i > \mathbf{V}_p(S)$. Then $\frac{1}{p^i} > p^{\mathbf{V}_p(S)-i}\frac{r}{s}$ and by 3.8a) there exists $\frac{u}{v} \in \mathbb{Q} \cap (p^{\mathbf{V}_p(S)-i}\frac{r}{s}, \frac{1}{p^i})$, $\mathbf{v}_p(\frac{u}{v}) = 0$ and $\gcd(u, v) = 1$.

Then $1 > \frac{p^i u}{v} > \frac{p^{\mathbf{V}_p(S)} r}{s}$ and so $\frac{p^{i-\mathbf{V}_p(S)} su}{rv} > 1$.

$p \nmid rv$, and so by 4.2.3 $\mathbf{a}_S(rv) = 1$ and by 4.2 $\frac{p^{i-\mathbf{V}_p(S)} su}{rv} \in S$ and also $\frac{p^i u}{v} = \frac{p^{\mathbf{V}_p(S)} r}{s} \cdot \frac{p^{i-\mathbf{V}_p(S)} su}{rv} = \frac{p^i u}{v} \in S$.

Thus $\frac{p^i u}{v} \in T$ and $R_i \neq \emptyset$. $\square$

4.3.2 Lemma *Let p be a prime and $\frac{pr}{s} \in T$, $r, s \in \mathbb{N}$ and $p \nmid s$. Then for all $t \in \mathbb{N}$ such that $p \nmid t$ and $1 > \frac{pr}{t} \geq \frac{pr}{s}$ is $\frac{pr}{t} \in T$.*

Proof. The case of $t = s$ is trivial, and so let $t \neq s$.

$\frac{pr}{t} > \frac{pr}{s}$, so $\frac{s}{t} > 1$, $p \nmid t$ and by 4.2.3 $\mathbf{a}_S(t) = 1$. This implies $\frac{s}{t} \in S$ and $1 > \frac{pr}{t} = \frac{pr}{s} \cdot \frac{s}{t} \in T$. $\square$

4.4 Let S be full p-divisible semiring for a prime p; let $T, R, R_i, B_{pr}, \mathbf{V}_p(S)$ and $\beta(pr)$ be as in 4.3.

As shown in 4.3.2, for $pr \in R$ is $B_{pr} = \{\frac{pr}{s}, s \in \mathbb{N}, p \nmid s \text{ and } \frac{pr}{s} \geq \beta(pr)\}$.

For $i \geq \mathbf{V}_p(S)$ we can define $\mathbf{c}_i = \inf\{\beta(p^i r) \mid p^i r \in R_i\}$. By 4.3.1 $R_i \neq \emptyset$ and so $\mathbf{c}_i$ is a real number.

4.4.1 Lemma *Let $i \geq \mathbf{V}_p(S)$ and $x \in \mathbb{Q} \cap (0,1)$ such that $x \neq \mathbf{c}_i$ and $v_p(x) = i$. Then $x \in S$ if and only if $x > \mathbf{c}_i$.*

Proof. Let $x \in T$, $x \neq \mathbf{c}_i$, $v_p(x) = i$ and $x = p^i \frac{r}{s}$, $p \nmid r$, $p \nmid s$. Then $p^i r \in R_i$, and so $x \geq \beta(p^i r) \geq \mathbf{c}_i$. Because $x \neq \mathbf{c}_i$, it is $x > \mathbf{c}_i$.

On the other hand, let $x \in \mathbb{Q} \cap (0,1)$, $x > \mathbf{c}_i$, $v_p(x) = i$ and $x = p^i \frac{r}{s}$, where $p \nmid r$ and $p \nmid s$. From the definition of $\mathbf{c}_i$ follows that there exists $p^i u \in R_i$ such that $x \geq \beta(p^i u) = \frac{p^i u}{v} \geq \mathbf{c}_i$. Then $\frac{r}{s} \geq \frac{u}{v}$ and $\frac{rv}{su} \geq 1$. $p \nmid su$ implies $\mathbf{a}_S(su) = 1$ and $\frac{rv}{su} \in S$. Then also $x = \frac{p^i r}{s} = \frac{p^i u}{v} \cdot \frac{rv}{su} \in S$. □

4.4.2 Lemma *If $i \geq \mathbf{V}_p(S)$ then $\mathbf{c}_i > 0$.*

Proof. Clearly $\mathbf{c}_i \geq 0$. Assume that $\mathbf{c}_i = 0$. By 4.4.1 $\frac{p^i}{r} \in T$ and for all $r > p^i$, $p \nmid r$, is $\frac{r}{p^i} \notin S$, a contradiction with the definition of $\mathbf{a}_S(p^i)$ (see 4.2). □

4.4.3 Lemma *If $i, j \geq \mathbf{V}_p(S)$, then $\mathbf{c}_i \mathbf{c}_j = \mathbf{c}_{i+j}$.*

Proof. 1) $\mathbf{c}_i \mathbf{c}_j \geq \mathbf{c}_{i+j}$

$\mathbf{c}_i = \inf\{b_{p^i r}; p^i r \in R_i\}$ and so there exists a sequence $x_k \in \{b_{p^i r}, p^i r \in \mathbf{R}_i\}$ such that $\lim x_k = \mathbf{c}_i$. Similarly there exists a sequence $y_k \in \{b_{p^j s}, p^j s \in \mathbf{R}_j\}$ such that $\lim y_k = \mathbf{c}_j$.

Now, $\mathbf{v}_p(x_k y_k) = i + j$, $x_k y_k \geq \mathbf{c}_{i+j}$ and $\mathbf{c}_i \mathbf{c}_j \geq \mathbf{c}_{i+j}$.

2) $\mathbf{c}_i \mathbf{c}_j \leq \mathbf{c}_{i+j}$.

$M_i = \{q, q \in \mathbb{Q}, \mathbf{v}_p(q) = i\}$ is a dense set in $\mathbb{Q}$ (see 3.8a)). So there exists a sequence $x_k \in M_i, 0 < x_k < \mathbf{c}_i$, $k \in \mathbb{N}$, such that $\lim x_k = \mathbf{c}_i$. Similarly there exists a sequence $y_k \in \{q, q \in \mathbb{Q}, \mathbf{v}_p(q) = j\}$, $k \in \mathbb{N}$, such that $0 < y_k < \mathbf{c}_j$ and $\lim y_k = \mathbf{c}_j$.

Now, by 4.4.1 $x_k, y_k \notin T$, (because S is full) $\frac{1}{x_k} \frac{1}{y_k} \in S$, thus $\frac{1}{x_k y_k} \in S$, and so $x_k y_k \notin T$.

$x_k y_k \in \mathbb{Q} \cap (0,1)$, $\mathbf{v}_p(x_k y_k) = i + j$, by 4.4.1 $x_k y_k \leq \mathbf{c}_{i+j}$, and so $\mathbf{c}_i \mathbf{c}_j \leq \mathbf{c}_{i+j}$. □

4.5 Let S be full p-divisible semiring for a prime p; let $\mathbf{V}_p(S)$ be as in 4.3 and $\mathbf{c}_i$ as in 4.4.

$\mathbf{c}_i^{i+i} = \mathbf{c}_{i+1}^i$ and so there exists $x \in \mathbb{R}$ such that $\mathbf{c}_i = x^i$ for all $i \geq \mathbf{V}_p(S)$. Let's denote $\mathbf{X}_p(S) = x$.

4.5.1 Lemma *Let there exist $i \geq \mathbf{V}_p(S)$ such that $\mathbf{c}_i \in S$. If $\mathbf{c}_j \in \mathbb{Q}$ for some $j \geq \mathbf{V}_p(S)$ then $\mathbf{c}_j \in S$. all $j \geq \mathbf{V}_p(S)$.*

Proof. If $\mathbf{c}_j \in \mathbb{Q} \setminus S$, then $\frac{1}{\mathbf{c}_j} \in S$ and also $\frac{1}{\mathbf{c}_j^i} = \frac{1}{\mathbf{c}_{ij}} \in S$, a contradiction with $\mathbf{c}_{ij} = c_i^j \in S$. □

4.5.2 Lemma *One of the following statements holds:*
a) Let $i \geq \mathbf{V}_p(S)$ and $x \in \mathbb{Q} \cap (0,1)$, $\mathbf{v}_p(x) = i$. Then $x \in S$ if and only if $x \geq \mathbf{c}_i$.
b) Let $i \geq \mathbf{V}_p(S)$ and $x \in \mathbb{Q} \cap (0,1)$, $\mathbf{v}_p(x) = i$. Then $x \in S$ if and only if $x > \mathbf{c}_i$.

Proof. Easy from 4.4.1 and 4.5.1. □

4.5.3 Lemma *One of the following statements holds:*
a) Let $x \in \mathbb{Q} \cap (0,1)$. Then $x \in S$ if and only if $\mathbf{v}_p(x) \geq \mathbf{V}_p(S)$ and $x \geq \mathbf{X}_p(S)^{\mathbf{v}_p(x)}$.
b) Let $x \in \mathbb{Q} \cap (0,1)$. Then $x \in S$ if and only if $\mathbf{v}_p(x) \geq \mathbf{V}_p(S)$ and $x > \mathbf{X}_p(S)^{\mathbf{v}_p(x)}$.

Proof. Combine 4.5.2 and 4.3. □

4.5.4 Lemma *One of the following statements holds:*
a) Let $x \in \mathbb{Q} \cap (1,\infty)$. Then $x \in S$ if and only if $\mathbf{v}_p(x) \geq 1 - \mathbf{V}_p(S)$ or $x > \mathbf{X}_p(S)^{\mathbf{v}_p(x)}$.
b) Let $x \in \mathbb{Q} \cap (1,\infty)$. Then $x \in S$ if and only if $\mathbf{v}_p(x) \geq 1 - \mathbf{V}_p(S)$ or $x \geq \mathbf{X}_p(S)^{\mathbf{v}_p(x)}$.

Proof. Easy from 4.5.3 and the fact that S is full. □

4.6 Statement *There is no full pq-divisible semiring S for p, q primes, $p \neq q$.*

Proof. Let S be a full pq-divisible semiring. Then S is full p-divisible semiring.

$\{x \in \mathbb{Q}, \mathbf{v}_p(x) = \mathbf{V}_p(S)$ and $\mathbf{v}_q(x) = 0\}$ is a dense set according to 3.8b), and so there exists $t \in \mathbb{Q}$ such that $\mathbf{v}_p(t) = \mathbf{V}_p(S)$, $\mathbf{v}_q(t) = 0$ and $(X_p(S))^{\mathbf{v}_p(t)} < t < 1$. It follows from 4.5.3 that $t \in S$.

But S is also full q-divisible semiring and $t \notin S$ again by 4.5.3 - a contradiction. $\square$

4.7 Let p be a prime, $x \in (0,1)$ and $k \in \mathbb{N}$. Define
$\mathbb{U}_p^k(x) = \{t \in \mathbb{Q} \cap (0,1), \mathbf{v}_p(t) \geq k \text{ and } t > x^{\mathbf{v}_p(t)}\} \cup \{t \in \mathbb{Q} \cap (1,\infty), \mathbf{v}_p(t) \geq 1-k \text{ or } t \geq x^{\mathbf{v}_p(t)}\}$,
$\mathbb{V}_p^k(x) = \{t \in \mathbb{Q} \cap (0,1), \mathbf{v}_p(t) \geq k \text{ and } t \geq x^{\mathbf{v}_p(t)}\} \cup \{t \in \mathbb{Q} \cap (1,\infty), \mathbf{v}_p(t) \geq 1-k \text{ or } t > x^{\mathbf{v}_p(t)}\}$,
$\mathbb{U}_p(x) = \mathbb{U}_p^1(x)$ and $\mathbb{V}_p(x) = \mathbb{V}_p^1(x)$.

4.7.1 Lemma *If $k \geq 2$ then $\mathbb{U}_p^k(x)$ (resp. $\mathbb{V}_p^k(x)$) is not a semiring.*

Proof. By 3.8a) there exists $\beta \in (x^k, 1) \cap \mathbb{Q}$ such that $\mathbf{v}_p(\beta) = b$ and there also exists $\alpha \in (1, \frac{1}{\beta}) \cap \mathbb{Q}$ such that $\mathbf{v}_p(\alpha) = 1 - b$.

$\alpha, \beta \in \mathbb{U}_p^k(x)$ (resp. $\alpha, \beta \in \mathbb{V}_p^k(x)$). But $\mathbf{v}_p(\alpha\beta) = 1$ and $\alpha \cdot \beta \notin \mathbb{U}_p^k(x)$ (resp. $\alpha \cdot \beta \notin \mathbb{V}_p^k(x)$), a contradiction. $\square$

4.7.2 Theorem *Let S be a full congruence simple subsemiring of $\mathbb{Q}^+$. Then there exists a prime p and $x \in (0,1)$ such that $S = \mathbb{U}_p(x)$ or $S = \mathbb{V}_p(x)$.*

Proof. Combine 3.7, 4.3, 4.5, 4.5.3, 4.5.4 and 4.7.1. $\square$

4.7.3 Observation $\mathbb{U}_p(x) = \{t \in \mathbb{Q} \cap (0,1), t > x^{\mathbf{v}_p(t)}\} \cup \{t \in \mathbb{Q} \cap (1,\infty), t \geq x^{\mathbf{v}_p(t)}\}$.
$\mathbb{V}_p^k(x) = \{t \in \mathbb{Q} \cap (0,1), t \geq x^{\mathbf{v}_p(t)}\} \cup \{t \in \mathbb{Q} \cap (1,\infty), t > x^{\mathbf{v}_p(t)}\}$.

4.7.4 Lemma $\mathbb{U}_p(x)$ *(resp. $\mathbb{V}_p(x)$) is a semiring.*

Proof. Easy. $\square$

4.7.5 Lemma $\mathbb{U}_p(x)$ *(resp. $\mathbb{V}_p(x)$) is archimedean and conical.*

Proof. By 2.10 we must prove that for every $n \in \mathbb{N}$ there exists $m \in \mathbb{N}$ such that $\frac{k}{n} \in S$ for every $k \geq m$.

Let $m > \frac{n}{x^{\mathbf{v}_p(n)}}$. For $k \geq m$ it holds that $\frac{k}{n} \geq \frac{m}{n} > x^{-\mathbf{v}_p(n)} \geq x^{\mathbf{v}_p(k)} \cdot x^{-\mathbf{v}_p(n)} = x^{\mathbf{v}_p(\frac{k}{n})}$, and so $\frac{k}{n} \in \mathbb{U}_p(x)$ (resp. $\frac{k}{n} \in \mathbb{V}_p(x)$). $\square$

4.7.6 Lemma *If there exists $a \in \mathbb{U}_p(x)$ (resp. $a \in \mathbb{V}_p(x)$) such that $a = x^{\mathbf{v}_p(a)}$, then $\mathbb{U}_p(x)$ (resp. $\mathbb{V}_p(x)$) is not bi-ideal simple.*

Proof. By 2.6 if $S = \mathbb{U}_p(x)$ (resp. $S = \mathbb{U}_p(x)$) is bi-ideal simple, then there exists $c \in S$ such that $a - ac \in S$. Since $a - ac \geq x^{\mathbf{v}_p(a-ac)} = x^{\mathbf{v}_p(a)} x^{\mathbf{v}_p(1-c)}$, it follows that $1 - c \geq x^{\mathbf{v}_p(1-c)}$. If $S = \mathbb{V}_p(x)$ then $1 - c \in S$ and so $1 \in S$, a contradiction.

So $S = \mathbb{U}_p(x)$, $1-c = x^{\mathbf{v}_p(1-c)} \notin S$, $c \in S$, but then $\mathbf{v}_p(c) \geq 1$, $\mathbf{v}_p(1-c) = 0$ and $1 - c = x^0 = 1$, a contradiction. □

4.7.7 *The following conditions are equivalent:*
1) $x = p \cdot (\frac{k}{l})^{\frac{1}{i}}$, where $k, l \in \mathbb{N}$, $p \nmid k$, $p \nmid l$, $i \in \mathbb{Z}$.
2) There exists $a \in \mathbb{U}_p(x)$ such that $a = x^{\mathbf{v}_p(a)}$.
3) There exists $a \in \mathbb{V}_p(x)$ such that $a = x^{\mathbf{v}_p(a)}$.

Proof. Easy. □

4.8 Let p be a prime and $x \in (0, 1)$. Denote $\mathbb{T}_p(x) = \{t \in \mathbb{Q}^+, t > x^{\mathbf{v}_p(t)}\}$.

4.8.1 $\mathbb{T}_p(x)$ *is congruence-simple semiring.*

Proof. The proof that $\mathbb{T}_p(x)$ is archimedean and conical semiring is similar to the proofs of 4.7.4 and 4.7.5.

According to 2.6 we must prove that $\mathbb{T}_p(x)$ is bi-ideal-simple, i.e. that for all $a, b \in \mathbb{T}_p(x)$ there exists $c \in \mathbb{T}_p(x)$ such that $a - bc \in \mathbb{T}_p(x)$.

$w = a - x^{\mathbf{v}_p(a)} > 0$. Let $i \in \mathbb{N}$ be such that $i > \mathbf{v}_p(a) - \mathbf{v}_p(b)$ and $\frac{w}{b} > x^i$ ($x^i \searrow 0$ for $i \to \infty$, and so there exists such i).

According to 3.8a) there exists $c \in \mathbb{Q}$ such that $\mathbf{v}_p(c) = i$ and $\frac{w}{b} > c > x^i = x^{\mathbf{v}_p(c)}$, and so $c \in \mathbb{T}_p(x)$.

$\mathbf{v}_p(c) = i > \mathbf{v}_p(a) - \mathbf{v}_p(b)$ and so $\mathbf{v}_p(a) < \mathbf{v}_p(bc)$ and by 3.2 $\mathbf{v}_p(a - bc) = \mathbf{v}_p(a)$. Then $a - bc > a - w = x^{\mathbf{v}_p(a)} = x^{\mathbf{v}_p(a-bc)}$ and $a - bc \in \mathbb{T}_p(x)$. □

4.8.2 Lemma *If $\mathbb{T}_p(x) = \mathbb{T}_q(y)$, than $p = q$ and $x = y$.*

Proof. Easy (use 4.6). □

4.9 Corollary *a) Let S be a full congruence-simple subsemiring of $\mathbb{Q}^+$. Then there exists a prime p and $x \in (0,1)$, $x \neq p \cdot (\frac{k}{l})^{\frac{1}{i}}$ for $k, l \in \mathbb{N}$, $p \nmid k$, $p \nmid l$ and $i \in \mathbb{Z}$ such that $S = \mathbb{T}_p(x)$. The choice of p and x is unique.*

b) Let p be a prime and $x \in (0,1)$ such that $x \neq p \cdot (\frac{k}{l})^{\frac{1}{i}}$ for $kl \in \mathbb{N}$, $p \nmid k$, $p \nmid l$ and $i \in \mathbb{Z}$. Then $\mathbb{T}_p(x)$ is a full congruence simple semiring.

Proof. Combine 4.7.2, 4.7.6, 4.7.7, 4.8.1 and 4.8.2. □

4.10 Remark It is not hard to observe that if $p_1, p_2, \ldots, p_n$ are primes and $x_1, x_2, \ldots, x_n \in (0,1)$ then $\bigcap_{i=1}^n \mathbb{T}_{p_i}(x_i)$ is a congruence-simple semiring. It follows from 4.7.6 and 4.7.7 that the semiring $\mathbb{T}_p(x)$ is a maximal congruence-simple subsemiring of $\mathbb{Q}^+$ (i.e., if $S \subseteq T \subseteq \mathbb{Q}^+$ and T is a congruence-simple semiring, then $T = S$ or $T = \mathbb{Q}^+$).

Also, if $\{q_i \mid i \in I\}$ are primes and $\{y_i \in (0,1) \mid i \in I\}$ for some index set I and $S = \bigcap_{i \in I} \mathbb{T}_{q_i}(y_i)$ is a congruence-simple semiring, then there exist primes $p_1, p_2, \ldots, p_n$ and $x_1, x_2, \ldots, x_n \in (0,1)$ such that $S = \bigcap_{i=1}^n \mathbb{T}_{p_i}(x_i)$.

Thus, by taking the intersections of finitely many of $\mathbb{T}_p(x)$ we get congruence-simple semirings; every known (at least to the author) example of a congruence-simple subsemiring of $\mathbb{Q}^+$ is of this form.

Bibliography

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