Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

SVOČ

Vítězslav Kala

Jednoduché polookruhy

Katedra algebry

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

2009

Děkuji svému vedoucímu profesoru Kepkovi za zajímavé téma práce. Dále děkuji Jakubu Opršalovi za jeho cennou pomoc s úpravou diplomové práce v systému $\mathcal{AMS}$-TEX. Během psaní práce jsem byl podporovaný Grantovou agenturou Univerzity Karlovy, grant číslo 8648/2008.

Contents

Název práce: Jednoduché polookruhy
Autor: Vítězslav Kala
Katedra (ústav): Katedra algebry
Vedoucí práce: Prof. RNDr. Tomáš Kepka, DrSc.
E-mail vedoucího: kepka@karlin.mff.cuni.cz
Abstrakt: Známé tvrzení říká, že pokud je komutativní těleso konečně generované jako okruh, je konečné. Tato práce je věnovaná zobecnění tohoto tvrzení – problému, jestli je každý konečně generovaný ideálově jednoduchý komutativní polookruh aditivně idempotentní nebo konečný. Pomocí charakterizace ideálově jednoduchých polookruhů dokážeme, že tato otázka je ekvivalentní otázce, zda je každé komutativní parapolotěleso (polookruh, jehož multiplikativní pologrupa je grupou), které je konečně generované jako polookruh, aditivně idempotentní. V práci odvodíme řadu užitečných vlastností takovýchto parapolotěles a využijeme jich k vyřešení problému v jednogenerovaném případě. Na závěr uvedeme, jak je možné využít získaných poznatků o parapolotělesech k vyřešení dvougenerovaného případu pomocí zkoumání podpologrup $\mathbb{N}_0^m$.
Klíčová slova: polookruh, parapolotěleso, ideálově jednoduchý, konečně generovaný, aditivně idempotentní

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: A well-known statement says that if a commutative field is finitely generated as a ring, then it is finite. This thesis studies a generalization of this statement – problem, whether every finitely generated ideal-simple commutative semiring is additively idempotent or finite. Using the characterization of ideal-simple semirings we prove that this question is equivalent to the question, whether every commutative parasemifield (i.e., a semiring whose multiplicative semigroup is a group), which is finitely generated as a semiring, is additively idempotent. In the thesis we deduce various useful properties of such parasemifields and use them to solve the problem in the one-generated case. Finally, we mention a way of using obtained properties of parasemifields for the solution of the two-generated case via the study of subsemigroups of $\mathbb{N}_0^m$.
Keywords: semiring, parasemifield, ideal-simple, finitely generated, additively idempotent

Introduction

A classical fact states that a (commutative) field is finite provided that it is finitely generated as a ring. Now, a ring is finitely generated if and only if it is finitely generated as a semiring; a ring is ideal-simple if and only if it is congruence-simple. Of course, simple commutative rings are just fields and zero-multiplication rings of finite prime order. Consequently, every finitely generated simple commutative ring is finite.

On the other hand, setting $a \oplus b = \min(a, b)$ and $a \odot b = a + b$ for all $a, b \in \mathbb{Z}$, we get an infinite commutative semiring that is both ideal- and congruence-simple and that is two-generated. This semiring is additively idempotent and it is known that every infinite finitely generated congruence-simple commutative semiring is additively idempotent. However, it seems to be an open problem whether this remains true in the ideal-simple case. It was probably first formulated in [1, 14.6].

The thesis is concerned with the study of this problem. In Chapter I we collect standard definitions (mostly related to semirings) which are used throughout the text.

In Chapter II we study ideal-simple semirings. Using the characterization of these semirings, we reduce the question to a special case of semirings – those whose multiplicative semigroups are groups (such semirings are called parasemifields). We show that the following two statements are equivalent:

(a) Every infinite finitely generated ideal-simple commutative semiring is additively idempotent.

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

The Chapter II consists of original results published in the article [3].

In Chapter III we study parasemifields, especially those that are finitely generated as semirings. We solve the problem for one-generated parasemifields (in fact, there are no such parasemifields). This chapter consists of original results from the article [5], which was submitted for publication.

In Conclusion we mention some other results related to the problem and suggest a possible direction of further research which might eventually lead to a complete solution.

Chapter I
Basic definitions

Definition. A *semiring* is a non-empty set S supplied with two associative operations (addition and multiplication) where the addition is commutative and the multication distributes over the addition from both sides. I.e., for all $x, y, z \in S$ holds

(i) $x + (y + z) = (x + y) + z$;
(ii) $x(yz) = (xy)z$;
(iii) $x + y = y + x$;
(iv) $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$.

A semiring is a ring if the addition defines an abelian group, i.e., if further:

(v) there exists $0 \in S$ such that $x + 0 = x$ for all $x \in S$;
(vi) for all $x \in S$ there exists $-x \in S$ such that $x + (-x) = 0$.

Definition. A semiring S is *commutative* if for all $x, y \in S$ holds $xy = yx$.

Definition. A non-trivial semiring S is a *parasemifield* if the multiplication defines a non-trivial group, i.e.

(i) there exists $1 \in S$ such that $x1 = x = 1x$ for all $x \in S$;
(ii) for all $x \in S$ there exists $x^{-1} \in S$ such that $xx^{-1} = 1 = x^{-1}x$.

Definition. A non-trivial semiring S is a *semifield* if

(i) there exists an element $w \in S$ such that w is multiplicatively absorbing (i.e. $Sw = wS = w$);

(ii) the set $S \backslash \{w\}$ is a subgroup of the multiplicative semigroup of S (i.e., there exists $1 \in S \backslash \{w\}$ such that $x1 = x = 1x$ for all $x \in S \backslash \{w\}$; for all $x \in S \backslash \{w\}$ there exists $x^{-1} \in S \backslash \{w\}$ such that $xx^{-1} = 1 = x^{-1}x$).

Definition. Let S be a semiring. A non-empty subset T of S is a *subsemiring* of S if it is a semiring (in other words, T is closed under addition and multiplication).

Similarly we define a subparasemifield and a subsemifield.

Definition. Let S be a semiring. A non-empty subset I of S is an *ideal* if $(I + I) \cup SI \cup IS \subseteq I$, i.e., for all $a, b \in I, s \in S$ holds

(i) $a + b \in I$;
(ii) $sa \in I$, $as \in I$.

The semiring is called *ideal-simple* if S is non-trivial and $I = S$ whenever I is an ideal containing at least two elements.

Definition. Let S be a semiring. A relation $\rho \subseteq S \times S$ is an *equivalence* if it is

(i) reflexive ($(x, x) \in \rho$ for all $x \in S$);
(ii) symmetric (if $(x, y) \in \rho$ for $x, y \in S$ then $(y, x) \in \rho$);
(iii) transitive (if $(x, y), (y, z) \in \rho$ for $x, y, z \in S$ then $(x, z) \in \rho$).

An equivalence on S is a *congruence* if for all $x, y, z \in S$ such that $(x, y) \in \rho$ holds

(iv) $(x + z, y + z) \in \rho$;
(v) $(xz, yz) \in \rho, (zx, zy) \in \rho$.

A semiring S is called *congruence-simple* if there are just two congruences on S.

Definition. Let S be a semiring. A relation $\rho \subseteq S \times S$ is a *quasiordering* if it is reflexive and transitive.

A quasiordering on S is an *ordering* if it is antisymmetric, i.e., if $(x, y), (y, x) \in \rho$ for $x, y \in S$ then $x = y$.

A quasiordering on S is *stable* if for all $x, y, z \in S$ such that $(x, y) \in \rho$ holds $(x + z, y + z) \in \rho$ and $(xz, yz) \in \rho, (zx, zy) \in \rho$.

Definition. A semiring S is called *additively idempotent* if for all $x \in S$ holds $x + x = x$, and *multiplicatively idempotent* if for all $x \in S$ holds $xx = x$.

Definition. A semiring S is called *additively cancellative* if for all $x, y, z \in S$ such that $x + y = x + z$ holds $y = z$, and *multiplicatively cancellative* if for all $x, y, z \in S$ such that $xy = xz$ or $yx = zx$ holds $y = z$.

Definition. A semiring S is called *additively constant* if there exists $x \in S$ such that for all $y, z \in S$ holds $y + z = x$, *multiplicatively constant* if there exists $x \in S$ such that for all $y, z \in S$ holds $yz = x$.

Definition. A semiring S is called *semisubtractible* if for all $x, y \in S$ there exists $z \in S$ such that $x = y + z$ or $y = x + z$.

Definition. Let S be a semiring. An element $w \in S$ is called *additively neutral* if for all $x \in S$ holds $x + w = x$. An element $w \in S$ is called *multiplicatively neutral* if for all $x \in S$ holds $xw = x = wx$.

Definition. Let S be a semiring. An element $w \in S$ is called *additively absorbing* if for all $x \in S$ holds $x + w = w$. An element $w \in S$ is called *multiplicatively absorbing* if for all $x \in S$ holds $xw = w = wx$.

Definition. Let S be a semiring. The semiring is *generated* by a set $A \subseteq S$ if whenever $T \subseteq S$ is a semiring containing A, we have $T = S$. In this case we also say that A *generates* S.

Let k be a non-negative integer. A semiring S is said to be k*-generated* if there is a set A, $|A| = k$, which generates S, and there is no set B, $|B| < k$, which generates S.

A semiring S is said to be *finitely generated* if it is k-generated for some non-negative integer k.

Notation. We use the following (standard) notation:

$\mathbb{N}$ ... the set of all positive integers
$\mathbb{N}_0$ ... the set of all non-negative integers
$\mathbb{Z}$ ... the set of all integers
$\mathbb{Q}$ ... the set of all rational numbers
$\mathbb{Q}^+$ ... the set of all positive rational numbers
$\mathbb{Q}_0^+$ ... the set of all non-negative rational numbers
$\mathbb{R}$ ... the set of all real numbers
$\mathbb{R}^+$ ... the set of all positive real numbers
$\mathbb{R}_0^+$ ... the set of all non-negative real numbers

Chapter II

Finitely generated ideal-simple commutative semirings

1. Preliminaries

The following lemma is obvious.

1.1 Lemma. *The following conditions are equivalent for a ring R:*
(i) R is ideal-simple as a ring.
(ii) R is ideal-simple as a semiring.
(iii) R is congruence-simple as a ring.
(iv) R is congruence-simple as a semiring.
(And then R is called simple.)

Every two element semiring is both ideal- and congruence-simple and it is easy to see there are exactly ten two element semirings (up to isomorphism). The following eight of them are commutative:

$\mathbb{S}_1$

+	0	1
0	0	0
1	0	0

·	0	1
0	0	0
1	0	0

$\mathbb{S}_2$

+	0	1
0	0	0
1	0	0

·	0	1
0	0	0
1	0	1

$\mathbb{S}_3$

+	0	1
0	0	0
1	0	1

·	0	1
0	0	0
1	0	0

$\mathbb{S}_4$

+	0	1
0	0	0
1	0	1

·	0	1
0	1	1
1	1	1

$\mathbb{S}_5$

+	0	1
0	0	0
1	0	1

·	0	1
0	0	1
1	1	1

$\mathbb{S}_6$

+	0	1
0	0	0
1	0	1

·	0	1
0	0	0
1	0	1

$\mathbb{S}_7$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	0

$\mathbb{S}_8$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Notice that $\mathbb{S}_1$ and $\mathbb{S}_2$ are additively constant, $\mathbb{S}_3, \mathbb{S}_4, \mathbb{S}_5$ and $\mathbb{S}_6$ are additively idempotent and $\mathbb{S}_7$ and $\mathbb{S}_8$ are rings. Moreover, $\mathbb{S}_1, \mathbb{S}_3, \mathbb{S}_4$ and $\mathbb{S}_7$ are multiplicatively constant and $\mathbb{S}_2, \mathbb{S}_5, \mathbb{S}_6$ and $\mathbb{S}_8$ are multiplicatively idempotent.

The following lemma is easy to prove.

1.2 Lemma. *Let S be a non-trivial semiring containing an element w such that $T = S\backslash\{w\}$ is a subgroup of the multiplicative semigroup of S.*

(i) If w is multiplicatively neutral (i.e., $w = 1_S$), then T is a subsemiring of S.

(ii) If w is multiplicatively absorbing but not additively absorbing, then w is additively neutral (i.e., $w = 0_S$) and either S is a division ring or T is a subsemiring of S.

(iii) If $|S| \geq 3$ and w is neither multiplicatively neutral nor multiplicatively absorbing then there exists $v \in T$ such that $wx = vx$ and $xw = xv$ for every $x \in S$.

2. Preliminaries continued

Only commutative semirings will be dealt with in the rest of the chapter, and hence the word 'semiring' will always mean a commutative semiring.

Clearly, each parasemifield is ideal-simple (in fact, ideal-free). Also, every semifield is ideal-simple.

We have the following basic classification of ideal-simple semirings (see e.g. [1, 11.2]):

2.1 Theorem. *A semiring S is ideal-simple if and only if it is of at least (and then just) one of the following five types:*

(1) $S \simeq \mathbb{S}_1, \mathbb{S}_3, \mathbb{S}_4$;

(2) S is a zero-multiplication (i.e., $xy = 0$ for all $x, y \in S$) ring of finite prime order;

(3) S is a field;

(4) S is a proper semifield;

(5) S is a parasemifield.

2.2 Proposition. *(*[1, 14.3]) *Every infinite finitely generated congruence-simple semiring is additively idempotent.*

2.3 Proposition. ([1, 14.5]) *No infinite finitely generated ideal-simple semiring is additively cancellative.*

2.4 Example. (i) The parasemifield $\mathbb{Q}^+ \times \mathbb{Q}^+$ (where $\mathbb{Q}$ denotes the field of rational numbers) is ideal-simple but not congruence-simple.

(ii) Denote by W the set of real numbers of the form $m - n\sqrt{2}$, where m, n are non-negative integers and $m + n \geq 1$. Put $a \oplus b = \min(a, b)$ and $a \odot b = a + b$ for all $a, b \in W$. Then $W(\oplus, \odot)$ is an infinite finitely generated congruence-simple semiring that is not ideal-simple. This semiring is additively idempotent and multiplicatively cancellative.

3. Semifields

In the following three lemmas, let S be a non-trivial semiring and let $w \in S$ be such that $T = S \setminus \{w\}$ is a subgroup of the multiplicative semigroup $S(\cdot)$.

3.1 Lemma. *If $1_T w = w$ then $Sw = w$ (i.e., w is multiplicatively absorbing) and S is a semifield.*

Proof. If $aw = v \neq w$ for some $a \in T$, then $w = 1_T w = a^{-1}aw = a^{-1}v \in T$, a contradiction. Consequently, $Tw = w$ and it remains to show that $ww = w$.

Assume that $ww = u \in T$. Then $1_T = u^{-1}u = u^{-1}ww = ww = u$ according to the preceding part of the proof, and therefore $ww = 1_T$ and $a = a1_T = aww = ww = 1_T$ for every $a \in T$. Thus we have shown that $S = \{w, 1_T\}$ and that S has the following multiplication table:

	w	1_T
w	1_T	w
1_T	w	1_T

Therefore $w(w + 1_T) = ww + w1_T = 1_T + w$, a contradiction since $wz \neq z$ for every $z \in S$. □

3.2 Lemma. *Assume that $1_T w = z \in T$ and $ww \in T$. Then:*

(i) T is a subsemiring of S.

(ii) If $|T| = 1$ then $S \simeq \mathbb{S}_1, \mathbb{S}_3, \mathbb{S}_4, \mathbb{S}_7$.

(iii) If $|T| \geq 2$ then T is a parasemifield (and so T is infinite).

(iv) $aw = az$ for every $a \in T$.

(v) $ww = zz$.

(vi) $Sw \subseteq T$ and T is an ideal of S.

(vii) If $a \in T$ then either $w + a = z + a \in T$ or $w + a = w$ and $z + a = z$.

(viii) If $w + w \in T$ then $w + w = z + z$.

(ix) If $w + w = w$ then S is additively idempotent.

Proof. If $a, b \in T$ are such that $a+b = w$, then $w = a+b = a1_T + b1_T = (a+b)1_T = w1_T = z$, a contradiction. Thus $T + T \subseteq T$ and T is a subsemiring of S. Further, $aw = a1_T w = az, a \in T$, and $ww = ww1_T = wz = zz$. The rest is easy. □

3.3 Lemma. *Assume that $1_T w = z \in T$ and $ww = w$. Then*

(i) T is a subsemiring of S.

(ii) If $|T| = 1$ then $S \simeq \mathbb{S}_2, \mathbb{S}_5, \mathbb{S}_6, \mathbb{S}_8$.

(iii) If $|T| \geq 2$ then T is a parasemifield (and so T is infinite).

(iv) $z = 1_T$.

(v) $wv = v$ for every $v \in S$ (i.e., $w = 1_S$).

(vi) T is an ideal of S.

(vii) If $a \in T$ then either $w + a = 1_T + a \in T$ or $w + a = w$ and $1_T + a = 1_T$.

(viii) If $w + w \in T$ then $w + w = 1_T + 1_T$.

(ix) If $w + w = w$ then S is additively idempotent.

Proof. Similar to that of 3.2. □

3.4 Lemma. *Let S be a non-trivial semiring and let $w_1, w_2 \in S$ be such that both $T_1 = S \backslash \{w_1\}$ and $T_2 = S \backslash \{w_2\}$ are subgroups of the multiplicative semigroup $S(\cdot)$. Then either $w_1 = w_2$ or $|S| = 2$ and $S \simeq \mathbb{S}_2, \mathbb{S}_5, \mathbb{S}_6, \mathbb{S}_8$.*

Proof. Assume that $w_1 \neq w_2$. If $|S| = 2$ then $S = \{1_{T_1}, 1_{T_2}\}$, and hence S is multiplicatively idempotent. If $|S| \geq 3$ then $T_1 \cap T_2 \neq \emptyset$. Now, $w_1 \in T_2$ and there is $a \in T_2$ such that $w_1 a \in T_1 \cap T_2$. Moreover, $w_1 ab = 1_{T_1}$ for some $b \in T_1$ and $cw_1 = 1_{T_2}$ for some $c \in T_2$. Then $c1_{T_1} = cw_1 ab = 1_{T_2} ab = ab$ and $1_{T_2} 1_{T_1} = w_1 c 1_{T_1} = w_1 ab = 1_{T_1}$. Similarly we get $1_{T_2} 1_{T_1} = 1_{T_2}$, and therefore $1_{T_1} = 1_{T_2} = 1_T$ is a multiplicatively neutral element of S. Then every element from S has an inverse, and so S is a group, a contradiction (see 3.1 and 3.2). □

3.5 Proposition. *Let S be a non-trivial semiring and let $w \in S$ be such that the set $S \backslash \{w\}$ is a subgroup of $S(\cdot)$. Then S is a semifield (i.e., Sw=w) in each of the following cases:*

(1) $1_T w = w$;

(2) $ww = w$ and $1_T w \neq 1_T$;

(3) $S \not\simeq \mathbb{S}_1, \mathbb{S}_7$, S is not additively idempotent and $\mathbb{Q}^+$ is not isomorphic to a subsemiring of S;

(4) S is finite, $S \not\simeq \mathbb{S}_1, \mathbb{S}_7$ and S is not additively idempotent.

Proof. Combine 3.1, 3.2 and 3.3. □

4. Semifields continued

4.1. Let T be a parasemifield. Then $0 \notin T$; let $S = T \cup \{0\}, x + 0 = x = 0 + x$ and $x0 = 0 = 0x$ for every $x \in S$. In this way we get a semifield (containing T as a semiring), which will be denoted $\mathbb{X}(T)$ in the sequel.

4.1.1 Lemma. *(i)* $\mathbb{X}(T)$ *is additively idempotent (resp. additively cancellative) if and only if* T *is such.*

(ii) A subset M *of* $\mathbb{X}(T)$ *generates* $\mathbb{X}(T)$ *as a semiring if and only if* $0 \in M$ *and* $M \cap T$ *generates* T *as a semiring (then* $|M| \geq 2$*).*

(iii) $\mathbb{X}(T)$ *is a finitely generated semiring if and only if* T *is such.*

(iv) $\mathbb{X}(T)$ *is not a one-generated semiring; it is a two-generated semiring if and only if* T *is a one-generated semiring.*

Proof. Easy to see. □

4.2. Let $A(\cdot)$ be a non-trivial abelian group, $o \notin A$, $S = A \cup \{o\}$, $x + o = o = o + x$, $x \in S$; $a + a = a$ and $a + b = o$, $a, b \in A$, $a \neq b$. Moreover, $xo = o = ox$, $x \in S$. In this way we get an additively idempotent semifield which will be denoted as $\mathbb{V}(A(\cdot))$.

4.2.1 Lemma. *(i) A subset* M *of* $\mathbb{V}(A(\cdot))$ *generates* $\mathbb{V}(A(\cdot))$ *as a semiring if and only if* $M \cap A$ *generates* $A(\cdot)$ *as a semigroup.*

(ii) $\mathbb{V}(A(\cdot))$ *is a finitely generated semiring if and only if* $A(\cdot)$ *is a finitely generated group.*

(iii) $\mathbb{V}(A(\cdot))$ *is a one-generated semiring if and only if* $A(\cdot)$ *is a one-generated semigroup. This is equivalent to the fact that* $A(\cdot)$ *is a finite cyclic group.*

(iv) $\mathbb{V}(A(\cdot))$ *is generated by a two-element set containing the unit element if and only if* $A(\cdot)$ *is a finite cyclic group (see (iii)).*

Proof. Easy to see. □

4.3. Let T be a parasemifield, $o \notin T$, $S = T \cup \{o\}, x + o = o + x = xo = ox = o$ for every $x \in S$. In this way we get a semifield which will be denoted as $\mathbb{U}(T)$.

4.3.1 Lemma. *(i)* $\mathbb{U}(T)$ *is additively idempotent if and only if* T *is such.*

(ii) A subset M *of* $\mathbb{U}(T)$ *generates* $\mathbb{U}(T)$ *as a semiring if and only if* $o \in M$ *and* $M \cap T$ *generates* T *as a semiring (then* $|M| \geq 2$*).*

(iii) $\mathbb{U}(T)$ *is a finitely generated semiring if and only if* T *is such.*

(iv) $\mathbb{U}(T)$ *is not a one-generated semiring; it is a two-generated semiring if and only if* T *is a one-generated semiring.*

Proof. Easy to see. □

4.4. Let T be a parasemifield and let the multiplicative group $T(\cdot)$ be a proper subgroup of an abelian group $A(\cdot)$, $o \notin A$. Put $S = A \cup \{o\}$ and define

a) $x + o = o = o + x$, $x \in S$;

b) $a + b = o, a, b \in A, a^{-1}b \notin T$;

c) $c + d = (1_T + c^{-1}d)c(= (1_T + d^{-1}c)d), c, d \in A, c^{-1}d \in T$.

Moreover, put $xo = o = ox, x \in S$. In this way we get a semifield which will be denoted as $\mathbb{W}(T, A(\cdot))$.

4.4.1 Lemma. *(i) T is a subsemiring of $\mathbb{W}(T, A(\cdot))$.*

(ii) $\mathbb{W}(T, A(\cdot))$ is additively idempotent if and only if T is such.

(iii) A subset M of $\mathbb{W}(T, A(\cdot))$ generates it as a semiring if and only if $M \backslash \{o\}$ generates S.

Proof. Easy to see. □

4.4.2 Lemma. *If the semiring $\mathbb{W}(T, A(\cdot))$ is generated by $a_1, \dots, a_m \in A, m \geq 1$, then the factorgroup $A(\cdot)/T(\cdot)$ is generated by the cosets $a_1T, \dots, a_mT$ as a semigroup.*

Proof. Let $a \in A$. Then $a = b_1 + \cdots + b_n, n \geq 1, b_j = a_1^{k_{1,j}} \cdots a_m^{k_{m,j}}, k_{i,j} \geq 0$. If $b_{j_1}^{-1} b_{j_2} \notin T$ for some $1 \leq j_1 < j_2 \leq n$, then $b_{j_1} + b_{j_2} = o$ and so $a = o$, a contradiction. Thus $b_{j_1}^{-1} b_{j_2} \in T$, and so $b_j = c_j b_1, c_j \in T$. Then $a = cb_1, c = c_1 + \cdots + c_n$ and $aT = b_1T$. The rest is clear. □

4.4.3 Lemma. *Let $a_1, \dots, a_m \in A, m \geq 1$, be such that the factorgroup $A(\cdot)/T(\cdot)$ is generated by the cosets $a_1T, \dots, a_mT$ as a semigroup. Denote by B the subsemigroup of $A(\cdot)$ generated by the elements $a_1, \dots, a_m$. Then for every $a \in A$ there are $b \in B$ and $c \in T$ such that $a = bc$.*

Proof. Obvious. □

4.4.4 Lemma. *If $\mathbb{W}(T, A(\cdot))$ is a finitely generated semiring then T is also.*

Proof. Let the semiring be generated by $a_1, \dots, a_m \in A, m \geq 1$. Denote by B the subsemigroup of $A(\cdot)$ generated by these elements. Then $C = BB^{-1} \cap T$ is a finitely generated subgroup of $T(\cdot)$, and hence the subsemiring T_1 of T generated by C is a finitely generated semiring. It remains to show that $T = T_1$.

Let $a \in T$. Then $a = b_1 + \cdots + b_n, n \geq 1, b_j \in B, b_j = c_j b_1, c_j = b_j b_1^{-1} \in C$ (see the proof of 4.4.2), and therefore $a = cb_1, c = c_1 + \cdots + c_n \in T_1$. Of course, $b_1 = c^{-1}a \in B \cap T \subseteq C \subseteq T_1$ and so $a, b_1, \dots, b_n \in T_1$. □

4.4.5 Lemma. *$\mathbb{W}(T, A(\cdot))$ is a finitely generated semiring if and only if T is a finitely generated semiring and $A(\cdot)/T(\cdot)$ is a finitely generated group.*

Proof. Combine 4.4.2, 4.4.3 and 4.4.4. □

4.4.6 Remark. Assume that $\mathbb{W}(T, A(\cdot))$ is generated by a single element s as a semiring, denote $1_{\mathbb{W}} = 1_{\mathbb{W}(T,A(\cdot))}$. We have $s \in A$; $B = \{s, s^2, s^3, \dots\}$ is the subsemigroup of $A(\cdot)$ generated by s and $BB^{-1} = \{\dots, s^{-3}, s^{-2}, s^{-1}, 1_{\mathbb{W}}, s, s^2, s^3, \dots\}$ is the subgroup generated by s. Notice that $s \neq 1_{\mathbb{W}}$.

(i) For every $a \in A$ there are $m \geq 1$ and $1 \leq k_1 \leq \cdots \leq k_m$ such that $a = s^{k_1} + s^{k_2} + \cdots + s^{k_m} = s^{k_1} b$, $b = 1_{\mathbb{W}} + s^{k_2 - k_1} + \cdots + s^{k_m - k_1}$. Since $a \neq o$, we have $s^{k_2 - k_1}, \dots, s^{k_m - k_1} \in T$ and so $b \in T$. Moreover, if $a \in T$ then $s^{k_1} = ab^{-1} \in T$ and consequently $s^{k_1}, s^{k_2}, \dots, s^{k_m} \in T$.

(ii) It follows from (i) that $D = B \cap T \neq \emptyset$ and so D is a subsemigroup and $C = DD^{-1}$ a subgroup of $T(\cdot)$. Consequently, there is $n \geq 0$ such that $C = \{\dots, s^{-3n}, s^{-2n}, s^{-n}, 1_{\mathbb{W}}, s^n, s^{2n}, s^{3n}, \dots\}$.

(iii) Denote by T_1 the subsemiring of T generated by s^{-n} and s^n. It follows from (i) and (ii) that $T_1 = T$. Consequently, $n \geq 1$ and T is a two-generated semiring.

(iv) The factorgroup $A(\cdot)/T(\cdot)$ is generated by the coset sT as a semigroup. Thus $A(\cdot)/T(\cdot)$ is a finite cyclic group.

(v) Proceeding similarly as above, one can show that (iii) and (iv) remain true if $\mathbb{W}(T, A(\cdot))$ is generated by $1_{\mathbb{W}}$ and s as a semiring.

4.5 Theorem. *Let S be a semifield and let $w \in S$ be such that w is multiplicatively absorbing and $T = S\backslash\{w\}$ is a subgroup of $S(\cdot)$. Then just one of the following eight cases takes place:*

(1) $S \simeq \mathbb{S}_2$ (and w is bi-absorbing);

(2) $S \simeq \mathbb{S}_5$ (and w is additively neutral);

(3) $S \simeq \mathbb{S}_6$ (and w is bi-absorbing);

(4) T is a subparasemifield of S and $S \simeq \mathbb{X}(T)$ (and w is additively neutral);

(5) $|S| \geq 3$ and $S \simeq \mathbb{V}(T(\cdot))$ (and w is bi-absorbing and S is additively idempotent);

(6) T is a subparasemifield of S and $S \simeq \mathbb{U}(T)$ (and w is bi-absorbing);

(7) $T_1 = \{a \in T | a + 1_T \neq w\}$ is a subparasemifield of S, $T_1 \neq T$, and $S \simeq \mathbb{W}(T_1, T(\cdot))$ (and w is bi-absorbing);

(8) S is a field.

Proof. Easy (use 3.1, 3.2 and 3.3). □

5. Summary

5.1 Summary. Combining 2.1, 4.5, 4.1.1 (i), (iii), 4.2, 4.3.1 (i), (iii), 4.4.1(ii) and 4.4.4, we conclude that the following two assertions are equivalent:

(a) Every infinite finitely generated ideal-simple semiring is additively idempotent.

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

5.2 Remark. Let F be a field. If F is a finitely generated ring then F is finite. If F is finite then the multiplicative group $F\backslash\{0\}$ is cyclic, and hence F is generated by one element as a semiring.

5.3 Remark. Let S be a one-generated ideal-simple semiring. Combining 2.1, 4.5, 4.1.1(iv), 4.2.1(iii), 4.3.1(iv), 4.4.6 and 5.2, we get that one of the following cases takes place:

(1) $S \simeq \mathbb{S}_1, \mathbb{S}_3, \mathbb{S}_4$;

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

(3) S is a finite field;

(4) $S \simeq \mathbb{V}(A(\cdot))$, where $A(\cdot)$ is a non-trivial finite cyclic group;

(5) $S \simeq \mathbb{W}(T, A(\cdot))$, where T is a two-generated parasemifield and $A(\cdot)/T(\cdot)$ is a (non-trivial) finite cyclic group;

(6) S is a parasemifield.

Chapter III

Parasemifields

1. Preliminaries

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.

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 $\nu_S = id_S$.*

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) $\nu_T = id_T$ 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) $\eta_S = id_S$ 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 $\{a \in S | 2a = a\}$ 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. *$\rho_S = id_S$ 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 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 $\mathbb{Q}^+$, $r \neq id$. 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 $1_Q \in Q \subseteq \bigcap_{I \in Max(R)} I = J(R)$, 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 $\rho_S \restriction Q = id_Q$ then $\mathbb{Q}^+$ is isomorphic to a subsemiring of T, which is impossible by 1.18. Thus $\rho_S \restriction Q \neq id_Q$.

$Q \simeq \mathbb{Q}^+$ 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

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 $r = id$ 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. ([7]) 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 $P = \{ab^{-1} | a, b \in S\}$. 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 $a(1 + a + \cdots + a^{m-1}) = a + a^2 + \cdots + a^{m-1} + 1$, 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 $x = a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}$. Then $bx = a^{k-1}b + a^{k-2}b^2 + \cdots + ab^{k-1} + b^k = a^{k-1}b + a^{k-2}b^2 + \cdots + ab^{k-1} + a^k + z = ax + z$, 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 $(a + a^{-k})^{k+1} = a^{k+1} + (k+1)a^k a^{-k} + \cdots = (k+1) + z$ 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 $\lim_{m\to\infty} \frac{a_{m+1}}{a_m} = \lim_{m\to\infty} \frac{((n+1)m+n+1)!(nm)!m!}{(nm+n)!(n+1)!((n+1)m)!}$ $= \lim_{m\to\infty} \frac{((n+1)m+n+1)\dots((n+1)m+1)}{(nm+n)\dots(nm+1)(m+1)} = \frac{(n+1)^{n+1}}{n^n}$. 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 $\left(\binom{(n+1)m}{nm}1_S, (a + a^{-n})^{(n+1)m}\right) \in \mu_S$. 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)* $\eta_S = id_S$ *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 $r_0 + r_1 a + r_2 a^2 + \dots + r_m a^m, m \geq 0, r_i \in \mathbb{Q}^+ \cup \{0\}, \sum r_i \neq 0$.

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 $(r(a^j+a^{-1}), r_j a^j + a^{-1}) \in \mu_S$, and so $r_j a^j + a^{-1} \in R$. Then $g + a^{-1} = r\sum_{i \in I \setminus \{j\}} r_i a^i + (r_j a^j + a^{-1}) \in R$ 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. *$\rho_Q \restriction P = id_P$. 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 $\{x_1^{k_1} \cdots x_m^{k_m} | (k_1, \dots, k_m) \in \mathbb{N}_0^m\}$.

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

(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 $Q_a \subseteq K_a \subseteq P$.

(iii) Assume that the semiring S is finitely generated and $Q \cup R \subseteq K_a$ (i.e. $K_a = S$ by 4.8). Then $a^{-1} \in K_a$, and so $Q = Q_a = P$ by (ii). Consequently by 4.9, $P = S$, and so S is additively cancellative, a contradiction with 1.18.

4.21 Corollary. *Let S be a parasemifield that is 1-generated as a semiring. Then S is additively idempotent.*

Proof. Use 4.20(iii). □

4.22 Remark. *(cf. 4.21) 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 easily concludes 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 $m * n = m + n$, is a two-generated parasemifield (it is generated by the set $\{-1, 1\}$).

Conclusion

The thesis is concerned with the question whether every infinite (commutative) semiring that is finitely generated and ideal-simple is additively idempotent.

Hence, in Chapter II we studied such semirings. Using the characterization of ideal-simple semirings and the properties of related parasemifields and semifields, we reduced the problem to the question whether every parasemifield that is finitely generated as a semiring is additively idempotent.

To answer this question, in Chapter III we studied various properties of parasemifields. From them we were able to prove the hypothesis for 1-generated parasemifields.

The problem remains unsolved in general case. However, results in section III.4 related to the semiring Q seem to sugest a way of proceeding in the case with more generators via the study of subsemigroups of $\mathbb{N}_0^m$ (see remark III.4.19). In this way we were already able to prove the hypothesis in 2-generated case – see [4] and [6] for details.

For further information about semirings, the reader can consult [1] or [2].

References

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

[2] U. Hebisch and H. J. Weinert, *Halbringe – Algebraische Theorie und Anwendungen in der Informatik*, Teubner, Stuttgart, 1993.

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

[4] V. Kala and T. Kepka, *Commutative parasemifields finitely generated as semirings*, preprint.

[5] V. Kala, T. Kepka and M. Korbelář, *Notes on commutative parasemifields*, submitted.

[6] V. Kala, T. Kepka and M. Korbelář, *Notes on subsemigroups of* $\mathbb{N}_0^m(+)$, preprint.

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