FINITELY GENERATED ALGEBRAIC STRUCTURES WITH VARIOUS DIVISIBILITY CONDITIONS

J. JEŽEK, V. KALA AND T. KEPKA

Abstract. Infinite fields are not finitely generated rings. Similar question is considered for further algebraic structures, mainly commutative semirings. In this case, purely algebraic methods fail and topological properties of integral lattice points turn out to be useful. We prove that a commutative semiring that is a group with respect to multiplication, can be two-generated only if it belongs to the subclass of additively idempotent semirings; this class is equivalent to ℓ-groups.

1. Introduction

Finitely generated algebraic structures satisfying various divisibility and/or simplicity conditions show sometimes a tendency to have additional more or less strong properties. In fact, an archetypical example of such a situation is the following useful result of folklore type that is occasionally attributed to I. Kaplansky:

(A) A field is finite, provided that it is a finitely generated ring.

Now, (congruence/ideal-) simple commutative rings are just fields and zero multiplication rings of finite prime orders. Commutative division rings are fields. Therefore:

(B) A finitely generated commutative ring is finite, provided that it is simple or it is a division ring.

Notice that the multiplicative groups of finite fields are cyclic, and so these groups are one-generated semigroups and finite fields are one-generated semirings. Notice also that the additive groups of zero multiplication rings of prime order are cyclic, and so these groups are one-generated semigroups and the rings are one-generated semirings.

There are two immediate ways how to generalize (A). The first of them is an extension to the non-commutative case, of course. But this seems to be exceedingly difficult and the authors of the present note are not aware of any related result. The second way leads to commutative semirings, i.e.,

1991 *Mathematics Subject Classification.* 16Y60, 12K10.

Key words and phrases. finitely generated, simple, semiring, quasigroup.

The work is a part of the research project MSM0021620839, financed by MSMT. The first and the third authors were also partly supported by the Grant Agency of the Czech Republic, grant #201/09/0296, and the second author by the Grant Agency of Charles University, grant #8648/2008.

ring-like structures where addition and multiplication are commutative and associative (no neutral and/or absorbing elements assumed *a priori*).

In the present note we consider the case of commutative semirings. Although we obtain only a partial solution, the employed method may be of interest. Namely, the purely algebraic problem is linked with geometrical and topological properties of some sets of lattice points (see [1] and [6]).

A *semiring* is an algebraic structure with two associative binary operations, usually denoted by addition and multiplication, such that the addition is commutative and the multiplication distributes over the addition from either side. A semiring is said to be commutative if its multiplication is commutative (as well as the addition).

A *parasemifield* is a non-trivial commutative semiring, the multiplicative semigroup of which is a group. Familiar examples of such structures are the parasemifields $\mathbf{Q}^+$ and $\mathbf{R}^+$ of positive rational and positive real numbers (by adjoining 0 we get the semifields $\mathbf{Q}_0^+$ and $\mathbf{R}_0^+$ of non-negative rational and non-negative real numbers). Besides, additively idempotent parasemifields (i.e., those satisfying $2a = a$ for all a) are equivalent to the better known and popular lattice-ordered abelian groups (see [3] and [7]). The main result of this paper is Theorem 7.18, saying that a parasemifield is additively idempotent, provided that it is a two-generated semiring.

Define two binary operations $\oplus$ and $\odot$ on $\mathbf{Z}$ (the set and the ring of integers) by $m \oplus n = \min(m, n)$ and $m \odot n = m + n$ for all $m, n \in \mathbf{Z}$. Then $\mathbf{Z}(\oplus, \odot)$ becomes an additively idempotent parasemifield generated (as a semiring) by the two-element set $\{1, -1\}$. Moreover, $\mathbf{Z}(\oplus, \odot)$ is congruence-simple (and also ideal-simple). Quite different sort of ideal-simple semirings are the following ones: Let G be an abelian group (denoted multiplicatively) and let $o \notin G$ and $\mathbf{U}(G) = G \cup \{o\}$. Put $a + b = o$ and $ao = oa = a$ for all $a, b \in \mathbf{U}(G)$, the multiplication of G being extended. Notice that o is the only additively idempotent element of $\mathbf{U}(G)$ and that $\mathbf{U}(G)$ is a finitely generated semiring if and only if G is a finitely generated group. The semiring $\mathbf{U}(G)$ is congruence-simple if and only if $|G| = 1$. According to Corollary 14.3 of [2], the following is true:

(C) Every finitely generated congruence-simple commutative semiring is either finite or additively idempotent.

On the other hand, the following conjecture is an open problem:

(D) Every finitely generated ideal-simple commutative semiring is either finite or additively idempotent or it is a copy of the semiring $\mathbf{U}(G)$ for a finitely generated infinite abelian group G.

Put $\mathbf{Z}^* = \mathbf{Z} \cup \{1/2\}$ and extend the operations of the parasemifield $\mathbf{Z}(\oplus, \odot)$ by $1/2 \oplus 1/2 = 0$, $1/2 \oplus n = n \oplus 1/2 = n \oplus 0$, $1/2 \odot 1/2 = 1/2$ and $1/2 \odot n = n \odot 1/2 = n$ for all $n \in \mathbf{Z}$. We obtain a (unitary) division semiring $\mathbf{Z}^*(\oplus, \odot)$ that is finitely generated (namely by the set $\{1, -1, 1/2\}$) and that

is almost additively idempotent (all but one elements are additively idempotent). Furthermore, $\mathbf{Z}^*$ is neither congruence-simple nor ideal-simple. We have the following conjecture:

(E) Every finitely generated commutative division semiring is either finite or (almost) additively idempotent or it is a copy of $\mathbf{U}(G)$ for a finitely generated infinite abelian group G.

Now, it is not difficult to show (it may be used as a stimulating exercise) that commutative ideal-simple or division semirings are either finite or fields or copies of $\mathbf{U}(G)$ or additively idempotent or, finally, they are constructed in quite transparent ways from parasemifields. Then it turns out that both (D) and (E) are equivalent to:

(F) A parasemifield is additively idempotent, provided that it is a finitely generated semiring.

The statement (F) seems to be an open problem. Every parasemifield is infinite, it is not a one-generated semiring and, if it is not additively idempotent, then it contains a copy of $\mathbf{Q}^+$. The additively idempotent parasemifield $\mathbf{Z}(\oplus, \odot)$ is a two-generated semiring.

Theorem 7.18 of the present paper is just a partial solution of (F), but the method employed could possibly serve as a model for extensions. Namely, after a few steps the question is transferred to the investigation of additive subsemigroups of $\mathbf{N}_0^2$ (here, $\mathbf{N}$ denotes the semiring of positive integers and $\mathbf{N}_0$ that of non-negative integers). These subsemigroups are viewed as sets of lattice points; the question is then solved by using some elementary geometry of the corresponding convex envelopes inside $(\mathbf{Q}_0^+)^2$. An approach to a full solution of (F) could be to generalize the whole process to the n-generated case, for $n > 2$. However, the geometry then starts to cause troubles. Perhaps, deeper topological insight is needed.

The statement (C) and the (equivalent) conjectures (D) and (E) are generalizations of (B) which in turn follows immediately from (A); (F) is a semiring analogue of (A).

As concerns structures with one (binary) operation, the situation is completely different. Of course, the additive group of integers is a two-generated semigroup. Besides, avoiding associativity, we get even more: we also show in this paper that every countable groupoid can be embedded into a one-generated division groupoid, and every countable cancellation groupoid can be embedded into a quasigroup that is one-generated as a groupoid.

2. An elementary proof of statement (A)

Since the statement (A) will be used in what follows, we provide here one of its less known elementary proofs.

Let us start with a few easy observations concerning quite classical situation. Henceforth, let $Q \subseteq F$ be an extension of fields. Assume first that Q contains a subring R with $1_Q \in R \neq Q = R(R \setminus \{0\})^{-1}$ and $F = R[u_1, \ldots, u_n]$, where the elements $u_1, \ldots, u_n$ $(n \geq 1)$ are algebraic over Q.

For $i = 1, \ldots, n$ there are elements $a_{i,0}, \ldots, a_{i,m_i} \in R$ ($m_i \geq 1$) such that $a_{i,m_i} \neq 0 = a_{i,0} + a_{i,1}u_i + \cdots + a_{i,m_i}u_i^{m_i}$. Put $a = \prod_i a_{i,m_i}$, so that $0 \neq a \in R \subseteq S = R[a^{-1}] \subseteq Q$. We claim that the element a is contained in every non-zero prime ideal of the domain R. We proceed by contradiction to prove this claim. Therefore, let P be a prime ideal of R such that $a \notin P$ and $0 \neq b \in P$. Then $a^k \neq bb_0a^k + bb_1a^{k-1} + \cdots + bb_k \in P$ and $b^{-1} \neq b_0 + b_1a^{-1} + \cdots + b_ka^{-k}$ for all $k \geq 0$ and $b_0, b_1, \ldots, b_k \in R$. It follows that $b^{-1} \notin S$, $S \neq Q$ and S is not a field. Put $A = \sum Su_i^{l_i}$ where $1 \leq i \leq n$ and $0 \leq l_i < m_i$. We have $u_i^{m_i} = -a_{i,m_i}^{-1}a_{i,0} - a_{i,m_i}^{-1}a_{i,1}u_i - \cdots - a_{i,m_i}^{-1}a_{i,m_{i-1}}u_i^{m_{i-1}} \in A$ and it follows easily that $u_i^{k_i} \in A$ for all i and $k_i \geq 0$. Then $A = F$ and ${}_SF$ is a finitely generated S-module. The Q-module ${}_QQ$ is a direct summand of ${}_QF$, and so ${}_QQ$ is a homomorphic image of ${}_QF$. But any such homomorphism is at the same time an S-homomorphism and we conclude that ${}_SQ$ is a finitely generated S-module. Thus ${}_SQ = \sum Sc_jd_j^{-1}$ where $1 \leq j \leq t$, $c_j \in S$, $d_j \in S \setminus \{0\}$, and $Q = Qd_1 \ldots d_t \subseteq S$, a contradiction. We have proved our claim.

Now, more generally, assume that $F = Q[M]$ for a finite subset M of F. We want to show that F is algebraic over Q. Again, proceeding by contradiction, let $N \neq \emptyset$, $R_1 = Q[N]$ and $Q_1 = Q(N)$, where N is a transcendence base such that $N \subseteq M$. We have $R_1 \subseteq Q_1 \subseteq F = R_1[M \setminus N]$, F is algebraic over Q_1 and, due to the preceding observations, we are able to find an element $a_1 \in R_1$, $a_1 \neq 0$, such that a_1 is contained in all non-zero prime ideals of the polynomial ring R_1. In particular, $1 - a_1 \in R_1^* = Q \setminus \{0\}$ (the group of invertible elements), $a_1 \in Q$ and $a_1^{-1} \in R_1$. Thus R_1 has no non-zero prime ideals and R_1 is a field, a contradiction. We have proved that F is algebraic over Q. Then, of course, ${}_QF$ is a finitely generated Q-module. In particular, F is finite, provided that Q is such. If F is infinite and Q is the prime subfield of F, then $Q \simeq \mathbf{Q}$ and $R \simeq \mathbf{Z}$, where R is the prime subring. Since no non-zero integer is contained in all maximal ideals of the integral domain $\mathbf{Z}$, we get $F \neq R[M_1]$ for any finite subset M_1 of F. The statement (A) is thus proved.

3. One-generated division groupoids

By a *groupoid* we mean a non-empty set equipped with one binary operation (usually denoted as multiplication). A groupoid G is a *division groupoid* if $aG = Ga = G$ for every element $a \in G$. Notice that the class of division groupoids is closed under taking homomorphic images and cartesian products.

Theorem 3.1. *Every countable groupoid A is a subgroupoid of a groupoid C with the following properties:*

(i) *C is a one-generated groupoid;*
(ii) *C is a division groupoid;*
(iii) *C is congruence-simple;*
(iv) *if A is commutative then C is also commutative.*

Proof. Since every finite groupoid can be embedded into an infinite countable one, it is sufficient to prove the theorem under the assumption that A is infinite. Let $i \mapsto a_i$ be a bijection of $\mathbf{N}_0$ (the set of non-negative integers) onto A. Take an infinite countable set B disjoint with A and let $i \mapsto b_i$ be a bijection of $\mathbf{N}_0$ onto B. For $i, j \in \mathbf{N}_0$ put $f(i,j) = 2^{i+1}3^{j+1}$ and $g(i,j) = 5^{i+1}7^{j+1}$, so that f and g are two injective mappings of $\mathbf{N}_0 \times \mathbf{N}_0$ into $\mathbf{N}_0$ with disjoint ranges; observe that $f(i,j) > i$ and $g(i,j) > i$ for all i, j.

Define multiplication on the set $C = A \cup B$, extending the multiplication of A, by means of the following rules:

(1) $b_0 b_i = b_i b_0 = b_{i+1}$ for all i;
(2) $b_{i+1} b_{i+1} = a_i$ for all i;
(3) $b_i b_{f(i,j)} = b_{f(i,j)} b_i = a_j$ for all $i > 0$ and $j \geq 0$;
(4) $b_i b_{g(i,j)} = b_{g(i,j)} b_i = b_j$ for all $i > 0$ and $j \geq 0$;
(5) $a_0 b_0 = b_0 a_0 = b_0$;
(6) $a_{i+1} b_0 = b_0 a_{i+1} = a_i$ for all i;
(7) $a_i b_{f(i,j)} = b_{f(i,j)} a_i = a_j$ for all i, j;
(8) $a_i b_{g(i,j)} = b_{g(i,j)} a_i = b_j$ for all i, j;
(9) $xy = b_0$ in all the remaining cases.

One can easily check that the multiplication is correctly defined. Of course, A is a subgroupoid of B. The groupoid B is generated by the element b_0, since if a subgroupoid contains b_0 then by (1) it contains all the elements of B and then by (2) it contains all the elements of A.

Let $c, d \in C$. We are going to check that the equation $cx = d$ has at least one solution in C; the equation $xc = d$ will then have the same solution. If $c, d \in A$ then x exists by (7). If $c \in A$ and $d \in B$ then x exists by (8). If $c \in B$ and $d \in A$ then x exists by (3) and (6). Finally, if $c, d \in B$ then x exists by (1),(4) and (5).

Thus C is a division groupoid. Clearly, $xy = yx$ whenever $x, y \in C$ and either $x \notin A$ or $y \notin A$. Thus C is commutative whenever A is. It remains to prove that C is congruence-simple. Let $\rho \neq \mathrm{id}_C$ be a congruence of C; we need to show that $\rho = C \times C$.

Let us first prove that if $(a_k, a_l) \in \rho$ for some $k \neq l$ then $\rho = C \times C$. We have $(a_i, b_0) = (a_k b_{f(k,i)}, a_l b_{f(k,i)}) \in \rho$ for every i and it follows that $A \times A \subseteq \rho$. Since A is a subgroupoid of C and C is generated by b_0, we conclude that for every $b \in B$ there is an $a \in A$ with $(a, b) \in \rho$. Then, of course, $\rho = C \times C$.

Next we are going to prove that if $(b_k, b_l) \in \rho$ for some $k \neq l$ then $\rho = C \times C$. If $l = 0$, then $(b_{k+1}, b_1) = (b_k b_0, b_0 b_0) \in \rho$. Thus it is sufficient to restrict ourselves to the case when $k, l \geq 1$. There exist i, j such that $i \neq j$ and $f(k,i) \neq l \neq f(k,j)$. We have $(a_i, b_0) = (b_k b_{f(k,i)}, b_l b_{f(k,i)}) \in \rho$ and similarly $(a_j, b_0) \in \rho$. Thus $(a_i, a_j) \in \rho$ and we know already that this implies $\rho = C \times C$.

It remains to consider the case when $(a_k, b_l) \in \rho$ for some k, l. If $l \geq 1$ and $k \neq l$ then, choosing $i \geq 1$ with $g(k,i) > l$, we get $(b_i, b_0) = (a_k b_{g(k,i)}, b_l b_{g(k,i)}) \in \rho$, so that $\rho = C \times C$. If $k = l \geq 1$, then $(a_{k-1}, b_{k+1}) = (a_k b_0, b_k b_0) \in \rho$. Finally, if $l = 0$, then $(a_i, b_{f(k,i)+1}) = (a_k b_{f(k,i)}, b_0 b_{f(k,i)}) \in \rho$ for every i. □

4. One-generated quasigroups

A groupoid G is a *cancellation groupoid* if $ab \neq ac$ and $ba \neq ca$ for all $a, b, c \in G$ with $b \neq c$. If, moreover, G is a division groupoid, then G is called a *quasigroup*. By a *loop* we mean a quasigroup with a neutral element. Notice that every finite cancellation groupoid, and also every finite division groupoid, is a quasigroup; the class of cancellation groupoids is closed under taking subgroupoids and cartesian products.

It is quite easy to show that every (countable, commutative) cancellation groupoid is a subgroupoid of an infinite (countable, commutative) quasigroup.

Theorem 4.1. *Every countable cancellation groupoid A is a subgroupoid of a groupoid Q with the following properties:*

(i) *Q is a one-generated groupoid;*
(ii) *Q is a quasigroup;*
(iii) *if A is a loop then Q is a loop, with the same neutral element;*
(iv) *if A is commutative then C is also commutative.*

Proof. Clearly, we can assume that A is an infinite quasigroup. Let $i \mapsto a_i$ be a bijection of $\mathbf{N}_0$ onto A, such that if A has a neutral element then the neutral element of A is a_0. Take an infinite countable set B disjoint with A and let $i \mapsto b_i$ be a bijection of $\mathbf{N}_0$ onto B. Define multiplication, extending the multiplication of A, by means of induction and the following rules:

(1) $b_i b_i = b_{i+1}$ for all i;
(2) for $i \neq j$ let $b_i b_j = a_k$ where k is the least number such that $a_k \notin \{b_0 b_j, \dots, b_{i-1} b_j\} \cup \{b_i b_0, \dots, b_i b_{j-1}\}$. (Thus $b_i b_j$ is defined by induction on $i + j$.) Observe that $b_i b_j = b_j b_i$ for all i, j;
(3) $a_i b_j = b_j a_i = b_k$ where k is the least number such that $b_k \notin \{b_{j+1}\} \cup \{a_0 b_j, \dots, a_{i-1} b_j\} \cup \{a_i b_0, \dots, a_i b_{j-1}\} \cup \{b_j a_0, \dots, b_j a_{i-1}\} \cup \{b_0 a_i, \dots, b_{j-1} a_i\}$.

Thus $b_i b_j$ and $a_i b_j = b_j a_i$ are defined by induction on $i + j$. One can check easily that the multiplication on Q is defined correctly. Of course, A is a subgroupoid of Q. For a small illustration, the two tables in Fig. 1 show fragments of the multiplication table of Q.

One can easily check by induction on $i + j$ that $a_i b_j = b_j a_i$ and $b_i b_j = b_j b_i$ for all i, j. In particular, this proves (iv).

If a subgroupoid of Q contains the element b_0 then it contains all elements of B, since $b_i b_i = b_{i+1}$, and also all elements of A, since $b_0 b_{i+1} = a_i$. Thus B is generated by the element b_0. We get (i).

	b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7
b_0	b_1	a_0	a_1	a_2	a_3	a_4	a_5	a_6
b_1	a_0	b_2	a_2	a_1	a_4	a_3	a_6	a_5
b_2	a_1	a_2	b_3	a_0	a_5	a_6	a_3	a_4
b_3	a_2	a_1	a_0	b_4	a_6	a_5	a_4	a_3
b_4	a_3	a_4	a_5	a_6	b_5	a_0	a_1	a_2
b_5	a_4	a_3	a_6	a_5	a_0	b_6	a_2	a_1
b_6	a_5	a_6	a_3	a_4	a_1	a_2	b_7	a_0
b_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	b_8

	b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7
a_0	b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7
a_1	b_2	b_0	b_1	b_5	b_3	b_4	b_8	b_6
a_2	b_3	b_4	b_0	b_1	b_2	b_7	b_5	b_9
a_3	b_4	b_3	b_5	b_0	b_1	b_2	b_9	b_{10}
a_4	b_5	b_6	b_4	b_2	b_0	b_1	b_3	b_{11}
a_5	b_6	b_5	b_7	b_8	b_9	b_0	b_1	b_2
a_6	b_7	b_8	b_6	b_9	b_{10}	b_3	b_0	b_1
a_7	b_8	b_7	b_9	b_6	b_{11}	b_{10}	b_2	b_0

Fig. 1

One can easily verify that Q is a cancellation groupoid. By induction on i, $a_ib_i = b_0$ and $a_0b_i = b_i$ for all i. In particular, if a_0 is a neutral element of A then it is also a neutral element of Q. It remains to prove that Q is a division groupoid.

Let us prove by induction on i that $x \mapsto b_ix$ is a bijection of B onto $b_{i+1} \cup A$. We already know that the mapping is injective. Suppose that an element a_j of A is not in the range of this mapping, and let j be the least number with this property. There exists a number $k > j$ such that $\{a_0, \ldots, a_{j-1}\} \subseteq \{b_ib_0, \ldots, b_ib_{k-1}\}$. For all numbers $m \geq k$ we have $a_j \in \{b_0b_m, \ldots, b_{i-1}b_m\}$ by the definition of b_ib_m. It follows that at least one of the mappings $x \mapsto b_rx$, for $r < i$, is not injective, a contradiction.

One can prove in a similar way that for every number i, the mapping $x \mapsto a_ix$ is a bijection of B onto B and the mapping $x \mapsto b_ix$ is a bijection of A onto $B \setminus \{b_{i+1}\}$. □

Remark 4.2. The construction in the proof of Theorem 4.1 gives a little bit more than just the fact that the extension Q of A is one-generated: it can be shown that if A is a quasigroup then the quasigroup Q is generated by any element of $Q \setminus A$. Also, the last statement of the theorem can be strengthened: we have $xy = yx$ for all $x, y \in Q$ such that $\{x, y\} \not\subseteq A$.

Remark 4.3. A group is one-generated as a semigroup if and only if it is a finite cyclic group. The infinite cyclic group is two-generated, but not one-generated as a semigroup.

Remark 4.4. A groupoid satisfying the equation $(xy)(zu) = (xz)(yu)$ is called *medial*. According to Proposition 6.4.1 of [4], every finitely generated medial division groupoid is a quasigroup. On the other hand, $\mathbf{Z}(-)$ is a medial quasigroup that is generated by the number 1 as a groupoid.

5. Finitely generated subsemigroups of $\mathbf{N}_0^2(+)$

The sets $\mathbf{N}_0^2$ and $(\mathbf{Q}_0^+)^2$ will be considered in this section as semigroups with respect to addition (defined componentwise). The set $(\mathbf{Q}_0^+)^2$ is the

first quadrant of the rational plane; its elements will be called *points*. The elements of $\mathbf{N}_0^2$ will be called *lattice points*.

The *slope* $\sigma(k,l)$ of a point $(k,l) \neq (0,0)$ is defined in this way: If $k \neq 0$, put $\sigma(k,l) = l/k$; if $k = 0$, put $\sigma(k,l) = \infty$. As it is easy to see, we have $\sigma(k_1,l_1) \leq \sigma(k_2,l_2)$ if and only if $k_2 l_1 \leq k_1 l_2$. This observation will enable us to avoid dealing with fractions, so that it will be unnecessary to distinguish between points of finite and infinite slopes.

By a *ray* we mean a set R of points such that there exists a point $a \neq (0,0)$ with $R = \mathbf{Q}_0^+ a = \{ra : r \in \mathbf{Q}_0^+\}$; we say that R is generated by a. Clearly, every ray is generated by any of its points different from $(0,0)$; every ray is generated by a lattice point. The slope of a generating point (k,l) of R does not depend on the choice of (k,l) and is called the slope of R. Clearly, each ray is uniquely determined by its slope.

By an *angle* we mean a non-empty subset U of $(\mathbf{Q}_0^+)^2$ such that $\mathbf{Q}_0^+ U \subseteq U$ and whenever R_1, R_2, R_3 are rays such that $R_1 \subseteq U$, $R_3 \subseteq U$ and $\sigma(R_1) < \sigma(R_2) < \sigma(R_3)$ then $R_2 \subseteq U$. Clearly, every angle is a subsemigroup of $(\mathbf{Q}_0^+)^2$ containing the point $(0,0)$. For every subset X of $\mathbf{N}_0^2$, the least angle containing X will be denoted by $\measuredangle(X)$ and called the angle generated by X.

Proposition 5.1. *Let A be a subsemigroup of $\mathbf{N}_0^2(+)$. Then $\measuredangle(A) = \mathbf{Q}_0^+ A = \{r(a,b) : r \in \mathbf{Q}_0^+$ and $(a,b) \in A\}$.*

Proof. We need to prove that if (a_1,b_1) and (a_2,b_2) are two elements of $A \setminus \{(0,0)\}$ and $(p,q) \neq (0,0)$ is a lattice point such that $\sigma(a_1,b_1) < \sigma(p,q) < \sigma(a_2,b_2)$ then $(p,q) \in \mathbf{Q}_0^+ A$. If $a_2 = 0$, then a_1, b_2, p, q are positive integers, $p(a_1,b_1) + s(0,b_2) = a_1(p,q)$ for a positive rational number s, and hence there are positive integers k, l, t with $ta_1(p,q) = k(a_1,b_1) + l(0,b_2) \in A$; thus $(p,q) \in \mathbf{Q}_0^+ A$. Now, assume that $a_2 \neq 0$ and put $e = a_1 a_2 p$, $c = b_1 a_2 p$, $d = a_1 b_2 p$ and $f = a_1 a_2 q$, so that (e,c) is a lattice point generating the same ray as (a_1,b_1), (e,d) is a lattice point generating the same ray as (a_2,b_2) and (e,f) is a lattice point generating the same ray as (p,q); we have $c < f < d$. Put $r = (d-f)/(d-c)$, so that r and $1-r$ are positive rational numbers. There exists a positive integer n such that both nr and $n(1-r)$ are integers. Thus $nr(e,c) + n(1-r)(e,d) \in A$. One can easily check that $nr(e,c) + n(1-r)(e,d) = n(e,f)$, so that the point $n(e,f)$ belongs to $\mathbf{Q}_0^+ A$; this point generates the same ray as (p,q). □

Let U be an angle and $R \subseteq U$ be a ray. We say that R is a *border ray* of U if either $\sigma(R') \geq \sigma(R)$ for all rays $R' \subseteq U$ or $\sigma(R') \leq \sigma(R)$ for all rays $R' \subseteq U$; in the first case R is called the lower border ray and in the second case, the upper border ray of U. An angle is said to be *closed* if it has both the lower and the upper border. Clearly, an angle if closed if and only if it is generated by a pair of points different from $(0,0)$.

Proposition 5.2. *Let A be a non-trivial subsemigroup of $\mathbf{N}_0^2(+)$. Then A is a finitely generated semigroup if and only if $\measuredangle(A)$ is a closed angle.*

Proof. The direct implication is easy to see. In order to prove the converse, let A be a non-trivial subsemigroup of $\mathbf{N}_0^2$ such that the angle $C = \measuredangle(A)$ has both the lower border R_1 and the upper border R_2. There are elements $d_1 \in R_1 \cap A$ and $d_2 \in R_2 \cap A$. Easily, every element of C can be expressed as $rd_1 + sd_2$ for some $r, s \in \mathbf{Q}_0^+$. Put $D = \{rd_1 + sd_2 : r, s \in \mathbf{Q}_0^+,\ r \leq 1,\ s \leq 1\} \cap \mathbf{N}_0^2$, so that D is a finite subset of $\mathbf{N}_0^2$.

Let $a \in A$. Since $a \in C$, we have $a = r_1d_1 + r_2d_2$ for some $r_1, r_2 \in \mathbf{Q}_0^+$. We have $r_1 = s_1 + k$ and $r_2 = s_2 + l$ for some $k, l \in \mathbf{N}_0$ and $s_1, s_2 \in \mathbf{Q}_0^+$ such that $s_1 \leq 1$ and $s_2 \leq 1$. Put $c = s_1d_1 + s_2d_2$. Since $a = c + kd_1 + ld_2$ where a and $kd_1 + ld_2$ belong to N_0^2, we have $c \in D$. Thus every element a of A can be expressed as $c + kd_1 + ld_2$ for some $c \in D$ and some $k, l \in \mathbf{N}_0$.

For every $c \in D$ put $N_c = \{(k, l) \in \mathbf{N}_0^2 : c + kd_1 + ld_2 \in A\}$. Clearly, if $(k, l) \in N_c$ then $(k', l') \in N_c$ for all $(k', l') \in \mathbf{N}_0^2$ such that $k' \geq k$ and $l' \geq l$. Denote by M_c the set of the pairs $(k, l) \in N_c$ such that whenever $(k', l') \in N_c$ where $k' \leq k$ and $l' \leq l$, then $(k, l) = (k', l')$. Clearly, for every pair $(k, l) \in N_c$ there exists at least one pair $(k', l') \in M_c$ such that $k' \leq k$ and $l' \leq l$.

Let $c \in D$. It is easy to see that for every $k \in \mathbf{N}_0$ there exists at most one l such that $(k, l) \in M_c$; if $(k_1, l_1) \in M_c$ and $(k_2, l_2) \in M_c$ where $k_1 < k_2$ then $l_1 > l_2$. Thus if $k_0 < k_1 < k_2 < \ldots$ is an increasing sequence of non-negative integers for which there exist l_i with $(k_i, l_i) \in M_c$, then $l_0 > l_1 > l_2 > \ldots$. Consequently, any such sequence is finite. It follows that there exists a positive integer K such that $k < K$ whenever $(k, l) \in M_c$. Quite similarly, there exists a positive integer L such that $l < L$ whenever $(k, l) \in M_c$. This shows that the set M_c is finite.

Put $E = \{d_1, d_2\} \cup \bigcup_{c \in D} \{c + kd_1 + ld_2 : (k, l) \in M_c\}$. Taking into account the preceding part of this proof, we conclude easily that the semigroup A is generated by E. Since D is finite and each M_c is finite, the set E is finite. Thus A is finitely generated. □

A subsemigroup B of a commutative semigroup $A(+)$ is said to be *pure* if $a \in B$ whenever $a \in A$ and $na \in B$ for a positive integer n.

Proposition 5.3. *Let A be a pure subsemigroup of $\mathbf{N}_0^2(+)$ containing $(0, 0)$. If there exists an element $b \in A \setminus \{(0, 0)\}$ such that $a - b \in A$ whenever $a \in A$ and $a - b \in \mathbf{N}_0^2$, then A is finitely generated.*

Proof. Denote by B the set of the elements $b \in A$ such that $a - b \in A$ whenever $a \in A$ and $a - b \in \mathbf{N}_0^2$. Suppose that $B \neq \{0, 0\}$ and A is not finitely generated.

If both $(1, 0) \in A$ and $(0, 1) \in A$, then $A = \mathbf{N}_0^2$ and A is finitely generated, a contradiction. Thus either $(1, 0) \notin A$ or $(0, 1) \notin A$. From the reason of symmetry it is sufficient to consider the case $(1, 0) \notin A$.

Claim 1. $A \cap \mathbf{N}_0(1, 0) = \{(0, 0)\}$. This follows from the fact that A is pure.

Claim 2. B is a pure subsemigroup of $\mathbf{N}_0^2(+)$; if $a, b \in B$ are such that $a - b \in \mathbf{N}_0^2$, then $a - b \in B$. This can be checked easily.

Claim 3. $B \cap \mathbf{N}_0(1,0) = \{(0,0)\} = B \cap \mathbf{N}_0(0,1)$. The first equality follows from Claim 1, since $B \subseteq A$. Suppose that $(0,1) \in B$. Then $(r,s) \in A$ implies $(r,0) \in A$; since $(1,0) \notin A$ and A is pure, we conclude that $A = \mathbf{N}_0(0,1)$ and hence A is finitely generated, a contradiction. We get $(0,1) \notin B$. Consequently, $B \cap \mathbf{N}_0(0,1) = \{(0,0)\}$.

In the rest of the proof let $b = (k,l) \in B \setminus \{(0,0)\}$ be such that $k + l$ is minimal. It follows from Claim 3 that $k \neq 0 \neq l$.

Claim 4. $B = \mathbf{N}_0 b$. Suppose, on the contrary, that $B \setminus \mathbf{N}_0 b$ is non-empty and let $b' = (k', l') \in B \setminus \mathbf{N}_0 b$ be such that $k' + l'$ is minimal. Again, $k' \neq 0 \neq l'$. We have $l'b - lb' = (l'k - lk', 0)$ and $lb' - l'b = (lk' - l'k, 0)$; since $(1,0) \notin A$, we get $kl' = k'l$. If $k < k'$ then $l < l'$ and $b' - b = (k' - k, l' - l) \in B$; by the minimality of $k' + l'$ we get $b' - b \in \mathbf{N}_0 b$, so that $b' \in \mathbf{N}_0 b$, a contradiction. Thus $k' \leq k$ and then $l' \leq l$. However, $k + l \leq k' + l'$ by the minimality of $k + l$ and it follows that $k = k'$ and $l = l'$. Hence $b' = b$, a contradiction with $b' \in B \setminus \mathbf{N}_0 b$.

Claim 5. B is a proper subset of A. Indeed, B is finitely generated (by Claim 4), while A is not.

Claim 6. $el < kf$ whenever $(e,f) \in A \setminus B$. We have $l \neq 0 \neq f$. If $el = kf$ then $l(e,f) = f(k,l) \in B$, so that $(e,f) \in B$ (since B is pure), a contradiction. If $el > kf$ then $(el - kf, 0) = l(e,f) - f(k,l) \in \mathbf{N}_0^2$ and, since $(k,l) \in B$, we get $(el - kf, 0) \in A$; but then $(1,0) \in A$ (since A is pure), a contradiction.

Claim 7. $(0,1) \in A$. By Claim 5 there exists an element $(e,f) \in A \setminus B$. By Claim 6, $el < kf$. Hence $(0, kf - el) = k(e,f) - e(k,l) \in \mathbf{N}_0^2$, so that $(0, kf - el) \in A$ and thus $(0,1) \in A$.

Denote by C the set of the numbers $g \in \mathbf{N}_0$ such that $g \leq k$ and $(g,h) \in A$ for at least one positive integer h. For every $g \in C$ denote by $p(g)$ the least positive integer with $(g, p(g)) \in A$. Denote by A' the subsemigroup of $\mathbf{N}_0^2$ generated by the finite set $\{(g, p(g)) : g \in C\} \cup \{(0,0)\}$.

Claim 8. $0 \in C$, $p(0) = 1$, $p(k) = l$, $(0,1) \in A'$, $(k,l) \in A'$ and $B \subseteq A' \subset A$. These are easy observations. We have $A' \neq A$, since A' is finitely generated.

Take $a = (r,s) \in A \setminus A'$ such that the sum $r + s$ is minimal. Clearly, $r \neq 0 \neq s$ and $(r,s) \notin B$.

Claim 9. $rl < sk$. If $rl = sk$ then $la = sb$ and $a \in B$, a contradiction. If $rl > sk$ then $la - sb = (rl - sk, 0) \in A$ and then $(1,0) \in A$, a contradiction again.

Claim 10. $r < k$. Suppose $k \leq r$, so that (by Claim 9) $l < s$. We have $a - b = (r - k, s - l) \in A$, since $b \in B$. But $r - k + s - l < r + s$ implies $a - b \in A'$ by the minimality of $r + s$ and hence $a = (a - b) + b \in A'$, a contradiction.

Since $r < k$ and $(r, s) \in A$, we have $r \in C$, $(r, p(r)) \in A'$, $p(r) \leq s$. Since $(0, 1) \in A'$, we get $(0, s - p(r)) \in A'$ and thus $a = (r, s) = (r, p(r)) + (0, s - p(r)) \in A'$, a contradiction. □

6. Division semirings, semifields, parasemifields

If it exists, the unique additively neutral element of a semiring S will be denoted by 0_S (so that $0_S + x = x$ for all $x \in S$). If it exists, the unique multiplicatively neutral element of S will be denoted by 1_S (so that $1_S x = x$ for all $x \in S$). A semiring S may also contain a unique additively absorbing element a ($a + x = a$) and/or a unique multiplicatively absorbing element o ($ox = o$).

A semiring S is a ring if the additive semigroup $S(+)$ is a group. A non-trivial commutative ring S is a field if the non-zero elements of S constitute a subgroup of the multiplicative semigroup $S(\cdot)$.

One can easily see that every additively cancellative commutative semiring S can be embedded into a commutative ring R such that $R = S - S = \{x - y : x, y \in S\}$; the ring R is unique up to an isomorphism over S and is called the *difference ring* of S.

By a *division semiring* we mean a semiring S such that $|SS| \geq 2$ and S contains an element w with $S \setminus \{w\} \subseteq Sa \cap aS$ for every $a \in S \setminus \{w\}$. According to this definition, fields are just the commutative division rings (if $|SS| = 1$, then two-element zero multiplication rings would make exeption).

By a *semifield* we mean a commutative semiring S containing a multiplicatively absorbing element w such that $S \setminus \{w\}$ is a subgroup of the multiplicative semigroup of S. A semifield is said to be *proper* if it is not a field. Clearly, every semifield is a division semiring.

By a *parasemifield* we mean a non-trivial commutative semiring S such that the multiplicative semigroup of S is a group. Clearly, every parasemifield is a division semiring. Note that every parasemifield is infinite.

By an *ideal* of a commutative semiring S we mean a non-empty subset I such that $(I+I) \cup SI \subseteq I$. A commutative semiring is said to be *ideal-simple* if it has no non-trivial proper ideals. It is easy to check that a commutative ring is an ideal-simple semiring if and only if it is an (ideal-)simple ring in the usual sense.

A commutative semiring S is *congruence-simple* if it has precisely two congruences, id_S and $S \times S$. It is immediately seen that a commutative ring is congruence-simple if and only if it is a simple ring in the usual sense.

For a commutative semiring S, define a relation ρ_S on S by $(a, b) \in \rho_S$ if and only if $a + s = b + s$ for at least one $s \in S$. Obviously, ρ_S is a congruence of the semiring S and the factor S/ρ_S is an additively cancellative semiring (ρ_S is the smallest congruence with this property).

Lemma 6.1. *Let S be a commutative semiring and $T = S/\rho_S$. If T is a finitely generated semiring, then T does not contain a subsemiring isomorphic with the parasemifield $\mathbf{Q}^+$.*

Proof. Suppose that T is finitely generated and that T contains a subsemiring $P \simeq \mathbf{Q}^+$. The set $T_1 = T1_P$ is a subsemiring of T with the unit element $1_{T_1} = 1_P$ and $P \subseteq T_1$. The semiring T_1 is finitely generated, since it is a homomorphic image of T. Now, consider the difference ring $R = T_1 - T_1$ of T_1. Then $1_R = 1_{T_1} = 1_P$, R is a finitely generated semiring and $Q = P - P$ is an isomorphic copy of the field $\mathbf{Q}$. If I is a maximal ideal of R, then $Q \cap I = \{0_R\}$ and hence Q can be embedded into the field R/I. But R/I is a finitely generated semiring and so R/I is a finite field while Q is infinite, a contradiction. □

Lemma 6.2. *Let S be a commutative semiring and $T = S/\rho_S$. If $w \in T$ is such that $w + w = w$, then $w = 0_T$ is additively neutral and multiplicatively absorbing in T.*

Proof. Just use the fact that T is additively cancellative. □

Lemma 6.3. *Let S be a finitely generated commutative semiring and let S contain a subsemiring $P \simeq \mathbf{Q}^+$ with $1_P = 1_S$. Then $\rho_S = S \times S$.*

Proof. It follows from 6.1 that the restriction of ρ_S to P is different from id_P. Since P is congruence-simple, we have $P \times P \subseteq \rho_S$. Consequently, $1_S/\rho_S$ is an additively idempotent element of S/ρ_S. It follows by 6.2 that $1_S/\rho_S$ is both additively neutral and multiplicatively absorbing in S/ρ_S. Thus $a/\rho_S = (a1_S)/\rho_S = a/\rho_S \cdot 1_S/\rho_S = 1_S/\rho_S$, $(a, 1_S) \in \rho_S$ for every $a \in S$ and $\rho_S = S \times S$. □

Proposition 6.4. *Let S be a finitely generated, congruence-simple commutative semiring. Then S is either finite or additively idempotent.*

Proof. See Corollary 14.3 of [2]. □

Proposition 6.5. *Let S be a finitely generated, additively cancellative commutative semiring. If S is either ideal-simple or congruence-simple, then S is a finite simple ring (i.e., S is either a finite field or a zero multiplication ring of finite prime order).*

Proof. Use 6.4 and Proposition 14.5 of [2]. □

Proposition 6.6. *No one-generated commutative semiring is a parasemifield.*

Proof. Suppose that there exists a parasemifield P that is generated by one element as a semiring. Since P is a finitely generated semiring, P has a maximal congruence r. The factor $Q = P/r$ is a one-generated, congruence-simple semiring and, of course, a parasemifield. Now Theorem 10.1 of [2], providing a classification of congruence-simple commutative semirings, can be applied. The first five cases listed in that theorem are easily excluded. So, the sixth case is the only remaining one. But then P is additively cancellative, a contradiction with 6.5. □

7. Two-generated parasemifields

Throughout this section, let P be a parasemifield that is generated by a set $\{x, y\}$ as a semiring (we have $x \neq y$ due to 6.6). We claim that P is additively idempotent. To prove this, we proceed by means of contradiction. Suppose that P is not additively idempotent, so that $1_P \neq 2_P = 1_P + 1_P$. Then the prime subparasemifield Q of P is a copy of the parasemifield $\mathbf{Q}^+$ of positive rational numbers. Denote by S the set of the elements $u \in P$ such that $Q \cap (P + u) \neq \emptyset$.

Lemma 7.1. (i) *S is a subsemiring of P.*
(ii) *If $u_1, \dots, u_n \in P$ are such that $u_1 + \dots + u_n \in S$, then all the elements $u_1, \dots, u_n$ belong to S.*
(iii) *$Q + P$ is a subsemiring of P.*
(iv) *$Q \subseteq S \cap S^{-1} \cap (Q + P)$.*

Proof. It is obvious. □

Lemma 7.2. *$Q + P = S^{-1}$.*

Proof. If $u = q_1 + v$ where $q_1 \in Q$, then $u^{-1} + q_1^{-1} v u^{-1} = q_1^{-1} \in Q$ and hence $u \in S^{-1}$. Conversely, if $u^{-1} + w = q_2 \in Q$ where $w \in P$, then $q_2^{-1} 1_P + q_2^{-1} w u = u$ and $u \in Q + P$. □

Lemma 7.3. *The set $T = S \cap S^{-1} = S \cap (Q + P) = Q + S = Q + T$ is a subsemiring of P and T is a parasemifield.*

Proof. We have $T = S \cap S^{-1} = S \cap (Q + P)$ and hence T is a subsemiring of P, since both S and $S^{-1} = Q + P$ are subsemirings. Clearly, T is a parasemifield and $Q \subseteq T \subseteq S$. Since S is a subsemiring, we have $Q + S \subseteq S$. The inclusion $Q + S \subseteq Q + P$ is obvious, and therefore $Q + T \subseteq Q + S \subseteq S \cap (Q + P) = T$. Finally, if $u \in T$, then $u = q + v$ for some $q \in Q$ and $v \in P$, the element $w = q/2 + v$ belongs to $Q + P$, we have $u = w + q/2$, $w \in S$, and so $w \in T$. Thus $T \subseteq Q + T$. □

Lemma 7.4. *The parasemifield T is additively cancellative.*

Proof. Let $u, v, z \in T$ be such that $u + z = v + z$. Then $u^{-1} z \in T$ and it follows easily from the definition of the subsemiring S that $u^{-1} z + w = 2_P^n$ for some $w \in P$ and some non-negative integer n. Now, $z + wu = 2^n u$ and hence $u + 2^n u = u + z + wu = v + z + wu = v + 2^n u$. If $n = 0$, then $2u = u + v$. If $n \geq 1$, then $2(u + 2^{n-1} u) = u + u + 2^n u = u + v + 2^n u = v + v + 2^n u = 2(v + 2^{n-1} u)$ and consequently $u + 2^{n-1} u = v + 2^{n-1} u$. Proceeding by induction, we get $2u = u + v$ anyway. Quite symmetrically, $2v = u + v$, and so $2u = 2v$ and, finally, $u = v$. □

Lemma 7.5. *If $u, v, z \in S$ are such that $u + z = v + z$, then $u + q = v + q$ for every $q \in Q$ (in particular, $u + 1_P = v + 1_P$).*

Proof. The elements $u + q$, $v + q$, $z + q$ belong to T by 7.3 and the result ensues from 7.4. □

Lemma 7.6. *If $u, v \in T$ and $z \in S$ are such that $u + z = v + z$, then $u = v$.*

Proof. We have $u + 1_P = v + 1_P$ by 7.5 and then we get $u = v$ by 7.4. □

Lemma 7.7. *Neither S nor T is a finitely generated semiring.*

Proof. First, T is an additively cancellative parasemifield, and hence T is not a finitely generated semiring by 6.5. Next, it follows from 7.6 that the restriction of the congruence ρ_S to T is the identity on T, and consequently $\rho_S \neq S \times S$. Now, S is not finitely generated by 6.3. □

Lemma 7.8. $P = SS^{-1} = S(Q + P)$.

Proof. We have $u^{-1}(u+1_P) = 1_P + u^{-1} \in Q + P$ for every $u \in P$, and hence the element $v = u(u + 1_P)^{-1}$ belongs to S by 7.2. Now, $u = v(u + 1_P) \in SS^{-1}$. □

Lemma 7.9. $T \neq S \neq P$.

Proof. Since P is a finitely generated semiring while S is not, we have $S \neq P$. Now it follows from 7.8 that $S^{-1} \not\subseteq S$, and hence $S \neq T$, since $T^{-1} = T$. □

Lemma 7.10. *If $u \in P$ and $n \geq 1$ are such that $u^n \in S$ ($u^n \in Q + P$, $u^n \in T$, resp.), then $u \in S$ ($u \in Q + P$, $u \in T$, resp.).*

Proof. First, assume that $u^n \in S$. Then $u^n + w = q^n$ for some $w \in P$ and $q \in Q$ and we have $uv + w = qv$, where $v = u^{n-1} + u^{n-2}q + \cdots + uq^{n-2} + q^{n-1} \in P$. Now, $u + wv^{-1} = q \in Q$ and $u \in S$.

If $u^n \in Q + P$, then $u^{-n} \in S$ by 7.2, and hence $u^{-1} \in S$ and $u \in Q + P$. Finally, if $u^n \in T = S \cap S^{-1}$, then $u \in T$. □

Put $A = \{(k, l) \in \mathbf{N}_0^2 : x^k y^l \in S\}$ and $B = \{(k, l) \in \mathbf{N}_0^2 : x^k y^l \in T\}$.

Lemma 7.11. (i) *$(0, 0) \in A$ and $\{(0, 0)\} \neq A \neq \mathbf{N}_0^2$.*
(ii) *A is a pure subsemigroup of $\mathbf{N}_0^2(+)$.*
(iii) *A is not a finitely generated semigroup.*

Proof. First, $(0, 0) \in A$ and A is a subsemigroup of $\mathbf{N}_0^2(+)$, since $1_P \in Q \subseteq S$ and S is closed under multiplication. The fact that S is a pure subsemigroup follows easily from 7.10. If M is a (non-empty) generating subset of the semigroup A, then $\{x^k y^l : (k, l) \in M\}$ is a generating subset of the semiring S (use 7.1(ii)), and hence M is infinite due to 7.7. Consequently, A is not finitely generated and it follows that $\{(0, 0)\} \neq A \neq \mathbf{N}_0^2$. □

Lemma 7.12. *The following two conditions are equivalent for $(k, l) \in \mathbf{N}_0^2$:*
(i) *$(k, l) \in B$;*
(ii) *$(k, l) \in A$ and $(m - k, n - l) \in A$ for every pair $(m, n) \in A$ such that $m \geq k$ and $n \geq l$.*

Proof. (i) implies (ii). We have $u = x^k y^l \in T$, $u^{-1} = x^{-k} y^{-l} \in S$, $v = x^m y^n \in S$ and $u^{-1}v = x^{m-k} y^{n-l} \in S$. But $(m - k, n - l) \in \mathbf{N}_0^2$, and so $(m - k, n - l) \in A$.

(ii) implies (i). We have $u = x^k y^l \in S$ and $u^{-1} = \sum_{i=1}^t x^{k_i} y^{l_i}$ for some $(k_i, l_i) \in \mathbf{N}_0^2$ $(1 \leq i \leq t)$. Then $1_P = uu^{-1} = \sum x^{k+k_i} y^{l+l_i}$ and it follows from 7.1(ii) that $(k + k_i, l + l_i) \in A$ for every i. Now, using (ii), we get $(k_i, l_i) \in A$, and hence $u^{-1} \in S$. Thus $u \in S \cap S^{-1} = T$. □

Lemma 7.13. *$(0, 0) \in B \subset A$ and B is a pure subsemigroup of $\mathbf{N}_0^2(+)$.*

Proof. Use 7.12, 7.9 and 7.10. □

Lemma 7.14. *Let $q_i \in \mathbf{Q}_0^+$ and $(k_i, l_i) \in A$ $(1 \leq i \leq t)$ be such that $(k, l) = \sum_{i=1}^t (q_i k_i, q_i l_i) \in \mathbf{N}_0^2$. Then $(k, l) \in A$.*

Proof. We have $q_i = r_i/s_i$ for suitable $r_i \in \mathbf{N}_0$ and $s_i \in \mathbf{N}$. Put $s = s_1 \dots s_t$. Then $sq_i \in \mathbf{N}_0$, $(sq_i k_i, sq_i l_i) \in A$ and $(sk, sl) = \sum (sq_i k_i, sq_i l_i) \in A$. Thus $(sk, sl) \in A \cap s\mathbf{N}_0^2 = sA$ and $(k, l) \in A$. □

Lemma 7.15. *Let $(k, l) \in A$, $u = x^k y^l \in S$ and $(k_i, l_i) \in \mathbf{N}_0^2$ $(1 \leq i \leq t)$ be such that $u^{-1} = \sum_{i=1}^t v_i$, where $v_i = x^{k_i} y^{l_i} \in P$. Then:*

(i) *$(k + k_i, l + l_i) \in A$ for every i.*

(ii) *$(k, l) \in B$ and $u \in T$, provided that there exist positive integers n_i with $((n_i - 1)k + n_i k_i, (n_i - 1)l + n_i l_i) \in A$ for every i.*

Proof. (i) is easy (see the second part of the proof of 7.12).

(ii) Put $n = \sum n_i$. Then $u^{-n} = (\sum v_i)^n$ can be written as $\sum_r s_r \prod_{i-1}^t v_i^{r_i}$ where r runs over the set of the t-tuples $r = (r_1, \dots, r_t) \in \mathbf{N}_0^t$ with $\sum r_i = n$, and $s_r \in \mathbf{N}$. We have $u^{n-1} = x^{(n-1)k} y^{(n-1)l}$ and $u^{-1} = u^{n-1} u^{-n}$. On the other hand, $u^{n-1} \prod_{i=1}^t v_i^{r_i} = x^{a_r} y^{b_r}$ where $a_r = (n-1)k + \sum_{i=1}^t r_i k_i$ and $b_r = (n-1)l + \sum_{i=1}^t r_i l_i$. Thus $u^{-1} = \sum_r s_r x^{a_r} y^{b_r}$ and, in order to show that $u^{-1} \in S$, it is sufficient to check that $(a_r, b_r) \in A$ for every r.

There are $m_i \in \mathbf{N}_0$ with $n = n_i + m_i$ and we have $((n-1)k + nk_i, (n-1)l + nl_i) = (n-1)(k, l) + n(k_i, l_i) = (n_i - 1)(k, l) + n_i(k_i, l_i) + m_i(k + k_i, l + l_i) \in A$ for every i. Finally, $(a_r, b_r) = (n-1)(k, l) + \sum r_i (k_i, l_i) = \sum (r_i/n)((n-1)(k, l) + n(k_i, l_i)) = \sum (r_i/n)((n-1)k + nk_i, (n-1)l + nl_i) \in \mathbf{N}_0^2$ and $(a_r, b_r) \in A$ by 7.14. □

Lemma 7.16. *The following two conditions are equivalent for all $(k, l) \in A$ and $(a, b) \in \mathbf{N}_0^2$:*

(i) *$((n-1)k + na, (n-1)l + nb) \in A$ for a positive integer n;*

(ii) *there are $r, s \in \mathbf{Q}^+$, $(k_i, l_i) \in A$ and $q_i \in \mathbf{Q}_0^+$ $(1 \leq i \leq t)$ such that $((r-s)k + ra, (r-s)l + rb) = \sum_{i=1}^t (q_i k_i, q_i l_i)$.*

Moreover, if these equivalent conditions are satisfied, then $(k + a, l + b) \in A$.

Proof. (i) implies (ii). We put $r = n$, $s = t = 1$, $k_1 = (n-1)k + na$, $l_1 = (n-1)l + nb$ and $q_1 = 1$. Moreover, $n(k + a, l + b) = (k, l) + ((n-1)k + na, (n-1)l + nb) \in A$ and hence $(k + a, l + b) \in A$, since A is a pure subsemigroup of $\mathbf{N}_0^2(+)$.

(ii) implies (i). We have $r = n/c$ and $s = m/c$ for suitable $n, m, c \in \mathbf{N}$. Then $((n-m)k + na, (n-m)l + nb) = c((r-s)k + ra, (r-s)l + rb) =$

$\sum(cq_ik_i, cq_il_i) \in \mathbf{Z}^2 \cap (\mathbf{Q}_0^+)^2 = \mathbf{N}_0^2$ and $((n-m)k+na, (n-m)l+nb) \in A$ by 7.14. Now, $((n-1)k+na, (n-1)l+nb) = ((n-m)k+na, (n-m)l+nb) + ((m-1)k, (m-1)l) \in A$. □

Lemma 7.17. *For every $(k,l) \in A \setminus B$ there exists at least one $(a,b) \in \mathbf{N}_0^2$ such that $(k+a, l+b) \in A$ and $((r-s)k+ra, (r-s)l+rb) \neq \sum_{i=1}^t (q_ik_i, q_il_i)$ for all $r, s \in \mathbf{Q}^+$, $(k_i, l_i) \in A$ and $q_i \in \mathbf{Q}_0^+$ $(1 \leq i \leq t)$. In particular, $(k+a, l+b) \notin \mathbf{Q}(k,l)$ and $(a,b) \notin \mathbf{Q}(k,l)$.*

Proof. The result follows by an easy combination of 7.15 and 7.16. If $(a,b) = q(k,l)$ for some $q \in \mathbf{Q}$, then $(k+a, l+b) = (q+1)(k,l)$ and $q > -1$, since $(k,l) \in A \setminus \{(0,0)\}$. Now, $q+1 \in \mathbf{Q}^+$ and $((r_0-s_0)k+r_0a, (r_0-s_0)l+r_0b) = (0,0)$ where $r_0 = 1$ and $s_0 = q+1$, a contradiction. □

Theorem 7.18. *Let P be a parasemifield that is two-generated as a semiring. Then P is additively idempotent.*

Proof. It follows from 7.11, 7.12 and 5.3 that $B = \{(0,0)\}$. Thus 7.17 can be reformulated as follows: For every $(k,l) \in A \setminus \{(0,0)\}$ there exists at least one $(c,d) \in A$ with $(c,d) - (k,l) \in \mathbf{N}_0^2$ such that for all $r, s \in \mathbf{Q}^+$, $r(c,d) - s(k,l) \notin \measuredangle(A) = \{\sum_{i=1}^t q_i(k_i, l_i) : (k_i, l_i) \in A, q_i \in \mathbf{Q}_0^+\}$.

Since A is not finitely generated, by 5.2 the angle $\measuredangle(A)$ has at most one border ray. If (c,d) is not on a border ray, then for $r = 1$ and all sufficiently small positive rational numbers s we have $r(c,d) - s(k,l) \in \measuredangle(A)$, a contradiction. Thus (c,d) is on the border ray, for every $(k,l) \in A \setminus \{(0,0)\}$. Now, choose (k,l) to be also on that border ray. Then $(c,d) = q(k,l)$ for some $q \in \mathbf{Q}^+$ and $2(c,d) - q(k,l) = (c,d) \in A$, a contradiction. □

References

[1] A. Barvinok, *A course in convexity,* Graduate studies in mathematics **54**, Amer. Math. Soc., Providence, R. A. 2002.

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

[3] M. R. Darnel, *Theory of lattice-ordered groups,* Marcel Dekker, Inc., New York, Basel, Hong Kong 1995.

[4] J. Ježek and T. Kepka, *Medial groupoids,* Rozpravy ČSAV, Řada mat. a přír. věd **93** (1983), 93 pp.

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

[6] E. Krätzel, *Lattice points,* Deutsches Verlag des Wissenschaften, Berlin and Kluwer Acad. Publishers, Dordrecht, Berlin, London 1988.

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

Jaroslav Ježek, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 18600 Praha 8, Czech Republic

E-mail address: jezek@karlin.mff.cuni.cz

Vítězslav Kala, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 18600 Praha 8, Czech Republic

E-mail address: vita211@gmail.com

Tomáš Kepka, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 18600 Praha 8, Czech Republic
E-mail address: kepka@karlin.mff.cuni.cz