Czech Technical University in Prague
Faculty of Electrical Engineering
Department of Mathematics

Habilitation Thesis

Simple and Commutative Semirings

Miroslav Korbelář

July 2021

Acknowledgements

I would like to express my deepest thanks to my family for their patience, permanent support and encouragement. Also, I would like to thank to my co-authors, friends and colleagues, especially to prof. RNDr. Pavel Pták, DrSc. for his valuable comments and discussions.

Contents

Chapter 1

Introduction

The concept of a semiring generalizes the notion of a ring, allowing the additive substructure to be only a commutative semigroup instead of an abelian group. In this way the semirings become a natural generalization of algebraic structures as rings or distributive lattices that are intrinsically quite different.

Classical examples of these objects are the semiring of natural numbers or the semiring of positive rational numbers. The main part of the theory of semirings is connected with modern algebra but their origin goes back to the works of Dedekind [18], Macaulay [80], Krull [72] and Nöther [93] in connection with the study of ideals of a ring. They also appeared in papers of Hilbert [43] concerning the axiomatization of natural and non-negative rational numbers. Semirings stayed for a long time outside the main interest as their structure is, in comparison with the rings, more general and hence harder to investigate. But, starting with the 70's, the recognition of their need and importance in applications brought a deeper research on them (currently there are several thousands of papers - a huge list of them is in [32]). Semirings appear in a natural way in computer science and serve as an algebraic tool in the theory of automata, the theory of formal languages, the optimization theory or the graph theory [8, 21, 34, 37, 74, 75]. Currently, the semirings are intensively studied in tropical geometry that may be viewed as a piece-wise linear version of the classical algebraic geometry, see e.g. [30, 47, 48]. Basic information on algebraic properties and applications of semirings can be found, e.g., in [35, 36, 42].

This habilitation thesis consists of an introductory text and a collection of selected research publications. It deals with two topics. The first one includes commutative ideal-simple semirings and related problems on the structure of finitely generated semirings. The second topic deals with congruence-simple semirings. In both cases we will mainly consider such semirings whose additive semigroup has some distinguished properties, in particular when this semigroup is idempotent.

Ideal- and congruence-simple semirings are two basic concepts that generalize the notion of a simple ring. In an ideal-simple semiring S every ideal I has either one element or $I = S$. Significant classes of such semirings are semifields and parasemifields, where the multiplicative part (up to at most one element) forms a group.

Most of the theory and applications of ideal-simple semirings concerns the commutative semirings. Commutative (para)semifields appear naturally in various parts of mathematics as in tropical mathematics [47, 81], in control theory and optimization [31, 85], in cluster algebras [62, 92] that are connected to mirror symmetries, polyhedral geometry, toric geometry or Teichmüller theory, in combinatorics [7, 73, 87] and other areas [32, 35, 36]. An important subclass of parasemifields are the idempotent ones that are nothing else but the lattice-ordered groups [105]. These groups arise in many parts of mathematics and are closely related to MV-algebras that are the algebraic counterparts of many-valued Łukasiewicz logic [20, 80, 91].

Commutative semirings in general appear in the ideal theory of commutative rings and number theory [41, 77, 83, 103], in the theory of ordered rings [101], as Grothedieck semirings of isomorphism classes [4, 40], in idempotent analysis [67] and other areas of mathematics [32, 35]. In spite of that, commutative semirings are still not well understood and even the structure of finitely generated objects remains still undiscovered.

The remaining topic of the thesis concerns congruence-simple semirings. These semirings (and semiring congruences) are studied for their basic structural rôle within the theory (see e.g. [32, 33, 35, 61, 88]). The classification of congruence-simple semirings was initiated in [23] and further investigated, e.g., in [24, 56, 66]. The finite cases were especially studied in [63, 89, 108]. In view of their complex structure, congruence-simple semirings are also suggested as suitable candidates for a post-quantum cryptography [22, 84, 107], i.e., for the protocols that might withstand attacks via quantum computing.

The thesis is organised as follows. Chapter 2 contains the basic terminology. Chapter 3 is devoted to ideal-simple semirings and related problems on the additive structure of semirings that are commutative and finitely generated ($\mathcal{CF}$). It summarizes main results proved in [57, 64, 69, 70, 71]. We present several conjectures from [64, 69, 70] that were motivated by a research on commutative ideal-simple semirings in [23, 53]. In the first set of partially equivalent conjectures it is assumed that if a semiring $S \in \mathcal{CF}$ is additively divisible (and, possibly, it has a unity) then S is additively idempotent. The second set of conjectures proposes that if the semiring $S \in \mathcal{CF}$ has some weaker forms of additive divisibility then S is additively torsion (both additively torsion and additively regular, resp.). We confirm these conjectures for the semirings with one generator. Further, we consider these conjectures on a point-wise level, i.e., we assume the corresponding properties and implications only for a single element a in a semiring $S \in \mathcal{CF}$. In this case we show that such implications hold, in terms of free objects in the variety of commutative semirings, only for a special set of elements in one-generated semirings. We also prove that every at most countable semigroup $A(+)$, in particular the rationals $\mathbb{Q}(+)$, can be embedded into the additive reduct of a one-generated semiring. This result shows that one-generated semirings are essentially different from commutative rings where this cannot happen. As a final result we show that every commutative parasemifield

$S \in \mathcal{CF}$ is additively idempotent. This generalizes the results proved in [49, 52, 54] and provides an answer to a question in [23] on ideal-simple semirings.

In Chapter 4 we recall the basic classification of congruence-simple semirings from [24] and provide examples of their application in cryptography that were described in [22, 107]. In [63] finite congruence-simple semirings were studied with the help of their semimodules. As a generalization of this approach we provide in [65] a characterization of a subclass of additively idempotent congruence-simple semirings with a bi-absorbing element in terms of their semimodules of a special type (o-characteristic semimodules). This result is, moreover, an analogy to a similar conclusion about congruence-simple semirings with a zero in [66]. We also show that o-characteristic semimodules are uniquely determined. Finally, in [65] we present a generalization of a result in [50] that concerns congruence-simple semirings of endomorphisms of semilattices.

Appendix A contains the publications attached to the thesis.

Chapter 2

Preliminaries

2.1 Semigroups

In the sequel we use a few notions of semigroup theory. By $\mathbb{N}$ ($\mathbb{N}_0$, resp.) we denote the set of all positive (non-negative, resp.) integers. Recall that a semigroup $A(+)$ is a non-empty set A with a binary associative operation $+$. For a positive integer $n \in \mathbb{N}$ and $c \in A$, put $nc = \underbrace{c + \cdots + c}_{n-\text{times}}$. An element $a \in A$ is called

- *neutral* $\Leftrightarrow a + x = x + a = x$ for every element $x \in A$,
- *absorbing* $\Leftrightarrow a + x = x + a = a$ for every element $x \in A$,
- *idempotent* $\Leftrightarrow a = a + a$,
- *torsion* $\Leftrightarrow$ the semigroup $\mathbb{N} \cdot a = \{ka \mid k \in \mathbb{N}\}$ is finite,
- *regular* $\Leftrightarrow$ there is $b \in A$ such that $a = a + b + a$,
- *completely regular* $\Leftrightarrow$ there is $b \in A$ such that $a = a + b + a$ and $a + b = b + a$.
- *divisible* (*uniquely divisible*, resp.) $\Leftrightarrow$ for every $n \in \mathbb{N}$ there is (a unique, resp.) $c \in A$ such that $a = nc$.

We assign such a notion to the semigroup A itself if every element of A has the respective property. A *semilattice* is a commutative and idempotent semigroup. A *monoid* is a semigroup with a (unique) neutral element.

Let us note that an element $a \in A$ is completely regular if and only if a lies in some subgroup of A. By adopting our definition, such a group is for instance the semigroup generated by elements a and b with the neutral element $e = a + b$. Hence an element $a \in A$ generates a subgroup of A (i.e., the semigroup $\mathbb{N} \cdot a$ is a group) if and only if a is completely regular and torsion.

Besides the regular and completely regular semigroups, further significant classes of semigroups are inverse semigroups (those regular semigroups where all idempotents mutually commute) and Clifford semigroups (those regular semigroups where every idempotent commutes with each element), for an overview see [45]. Clifford semigroups are also characterized as semilattices of groups. All these classes of semigroups provide various generalizations of the notion of a group.

Clearly, for commutative semigroups, all the four notions (to be regular, completely regular, inverse or Clifford) coincide.

2.2 Semirings

A *semiring* $S(+,\cdot)$ is an algebraic structure such that S is a non-empty set equipped with two binary operations $+$ and $\cdot$ such that

- $S(+)$ is a commutative semigroup,
- $S(\cdot)$ is a semigroup,
- $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$ for every $a,b,c \in S$.

A semiring is *commutative* if its multiplicative semigroup is commutative. In the definition we in general do not require any constants. However, the semirings often do have constants and the significant cases in this aspect are the following ones. The semiring S is said to have

- a *unity* $1_S \in S \Leftrightarrow S(\cdot, 1_S)$ is a monoid,
- a *zero* $0_S \in S \Leftrightarrow S(+, 0_S)$ is a monoid and 0_S is an absorbing element with respect to the multiplication,
- a *bi-absorbing element* $o_S \in S \Leftrightarrow o_S$ is an absorbing element with respect to both operations addition and multiplication.

A semiring S is called *additively constant* if there is an element $o \in S$ such that $a+b = o$ for all $a, b \in S$. In this case $o = o_S \in S$ is always a bi-absorbing element of the semiring S.

A semiring S is called a *parasemifield* if $S(\cdot)$ is a group and S is called a *semifield* if there is a multiplicatively absorbing element $w \in S$ such that the set $S \setminus \{w\}$ is a multiplicative group. By a *proper* semiring (semifield, resp.) we mean a semiring (semifield, resp.) that is not a ring.

In the investigation of the structural properties of any algebraic systems, simple objects play a very important rôle. For example, the classification of finite simple groups received a vast attention and is completely known.

The notion of simplicity for a given algebraic structure may in general depend on the choice of a significant property and often is related to homomorphic images of the given structure. For semirings, there are two principal concepts of simplicity - *congruence-simple* and *ideal-simple* semirings.

An *ideal* (*left ideal*, resp.) I of a semiring S is a non-empty set such that for all $a \in S$ and $x, y \in I$ is $ax, xa, x+y \in I$ ($ax, x+y \in I$, resp.).

A *congruence* $\varrho \subseteq S \times S$ on a semiring S is an equivalence such that $(a, b) \in \varrho$ implies both $(a+c, b+c) \in \varrho$ and $(ac, bc), (ca, cb) \in \varrho$ for all $a, b, c \in S$.

A semiring S is called *congruence-simple* if S has precisely two congruences, and *ideal-simple* if every ideal I of S has either only one element or $I = S$.

For rings these two notions coincide but for semirings they substantially differ. Ideal-simple semirings can be seen as an analogy to simple semigroups (that are defined also by ideals) while congruence-simple semirings are analogous to simple groups (that are also defined by congruences).

As an example of a semiring that is ideal-simple but not congruence-simple, let us consider the semiring $S = \mathbb{Q}^+ \times \mathbb{Q}^+$ with component-wise standard operations on the positive rationals $\mathbb{Q}^+$. On the other hand, the semiring $S = \{a - b\sqrt{2} \mid a, b \in \mathbb{N}_0\}$ with so called *tropical* addition $x \oplus y = \max\{x, y\}$ and multiplication $x \odot y = x + y$ for all $x, y \in S$ is congruence-simple but not ideal-simple.

In this thesis we will investigate properties of idempotency, regularity, torsion and divisibility within a semiring $S(+, \cdot)$ only with respect to its additive semigroup $S(+)$ (up to an exception in Theorem 4.2.1). Sometimes we will emphasize this fact with the word *additively.* So we call, for instance, an element $a \in S$ (additively) idempotent if a is idempotent within the semigroup $S(+)$. Similarly, we assign all these notions to the semiring S itself (e.g., we say that S is idempotent) if every element of S has the respective property.

Let $x_1, \ldots, x_n$ be a set of variables. By $\mathbb{N}[x_1, \ldots, x_n]$ we denote the semiring of all non-zero polynomials over these variables with non-negative integer coefficients. Obviously, the semiring $\mathbb{N}[x_1, \ldots, x_n]$ has a unity. By $F(x_1, \ldots, x_n)$ we denote the free semiring with the free basis $x_1, \ldots, x_n$ in the category of all commutative semirings. Hence $F(x_1, \ldots, x_n)$ consists of all those polynomials in $\mathbb{N}[x_1, \ldots, x_n]$ that have no constant terms. Thus, $F(x_1, \ldots, x_n)$ does *not* have a unity.

For a semiring S and a non-empty set $X \subseteq S$ we denote by $\langle X \rangle^+$ the subsemigroup of the semigroup $S(+)$ that is generated by the set X and by $\langle X \rangle$ the subsemiring of S that is generated by X. We say that a semiring S is finitely generated if there is a finite subset $Y \subseteq S$ such that $S = \langle Y \rangle$. In particular, S is one-generated if there is an element $w \in S$ such that $S = \{f(w) \mid f \in F(x)\}$ (because such a semiring is always commutative). For the sake of simplicity we denote by $\mathcal{CF}$ the class of all finitely generated commutative semirings.

Finally, as we will also deal with semimodules in Chapter 4, let us recall this notion. For a commutative semigroup $M(+)$, let us denote by $End(M)(+, \circ)$ the semiring of all endomorphisms of the semigroup $M(+)$ with the usual composition $(f \circ g)(m) = f(g(m))$ and point-wise addition $(f + g)(m) = f(m) + g(m)$ of maps $f, g \in End(M)$ for any $m \in M$.

Now, M is called a *(left) S-semimodule* for a semiring S if S acts on M via a semiring homomorphism $\Phi : S \to End(M)$. Such an action $\Phi(s)(m)$ of the element

$s \in S$ on the element $m \in M$ is usually abbreviated as sm. The semimodule M is called *faithfull* if Φ is a monomorphism and *minimal* if $|M| \geq 2$ and for every S-subsemimodule N of M such that $|N| \geq 2$ is $N = M$.

Obviously, every left ideal I of S is an S-semimodule with a natural action given by $\Phi(s)(m) = s \cdot m$, for $s \in S$ and $m \in I$. A left ideal I is *minimal* if it is minimal as the natural S-semimodule.

Chapter 3

Commutative ideal-simple semirings and related problems on finitely generated semirings

3.1 Commutative ideal-simple semirings

Most of the theory and applications of ideal-simple semirings are related to the commutative case. Commutative semirings are closely connected with the study of ideals in commutative algebra, theoretical arithmetics, number theory and with so called *tropical* mathematics. The tropical mathematics is nothing but commutative algebra that is based on tropical semirings instead on commutative rings. A typical example of such a semiring are the real numbers with maximum as the *additive* operation and the usual addition in the reals as the *multiplicative* operation. Tropical mathematics has a natural connection to algebraic geometry with growing development in this direction (see e.g. [16, 48, 86, 98]). Typical varieties here are the polyhedral complexes which have strong applications in enumerative algebraic geometry. Tropical mathematics is also useful in studying piece-wise linear functions in optimization problems (see e.g. [31, 78, 85]). Another interesting application of tropical mathematics is in computational phylogenetics [95, 100], where a phylogenetic tree of the genetic relationship is constructed from a given distance matrix.

The commutative (congruence- or ideal-) simple semirings were characterized and partially classified in [23]. A commutative ideal-simple semiring S with at least three elements falls precisely into one of the following cases:

- S is a zero-multiplication ring (i.e., $ab = 0$ for all $a, b \in S$) of finite prime order;
- S is a field;
- S is a proper semifield;
- S is a parasemifield.

This basic classification raised further fundamental structural questions on commutative semirings.

3.2 Conjectures related to idempotency

In this section we present several conjectures on finitely generated commutative semirings. These conjectures are related to each other and have the two following motivations.

The first motivation is connected with commutative ideal-simple semirings. To obtain a more detailed insight into them it is natural to start with finite or, rather, with finitely generated cases. Finite cases in the basic classification include finite fields, zero-multiplication rings of finite prime order, the trivial semiring and semifields that are either additively constant or additively idempotent [23, 3.2]. These cases do not seem to share any common features. On the other hand, by a classical result, no infinite field can be finitely generated as a (semi)ring. Hence, considering *finitely generated* cases in the basic classification that are *infinite*, one obtains only proper semifields or parasemifields. It was conjectured that such infinite cases have to be additively idempotent or additively constant (for the details, see [23, 49, 51, 53]).

The second motivation comes from a kind of a “folklore” theorem in the ring theory saying that a finitely generated commutative ring cannot contain the field $\mathbb{Q}$ of rationals. In this context a natural question suggests itself whether or not an analogous theorem remains true for semirings.

Motivated by these questions, a sequence of further conjectures on finitely generated commutative semirings was proposed in [64]. One of the key notions in these conjectures is the (additive) divisibility. This property has allowed to extend formulations of conjectures from ideal-simple semirings to arbitrary commutative semirings that are finitely generated.

The conjectures are listed below. Let us make a few comments to more explain their formulations. Note that the idempotency trivially implies the divisibility. Also, every parasemifield S is additively divisible as its unity 1_S has this property. This immediately follows from the fact that the unity 1_S is contained in the smallest (prime) subparasemifield P of S and such P either consists of a single element or it is isomorphic to the parasemifield $\mathbb{Q}^+$ of the positive rationals.

Further, the divisible structures (e.g., the divisible groups) are usually expected to be “large”. On the other hand, the finitely generated objects are usually “small”. In the case of the commutative semirings, the only way for these two properties to co-exist seems to be in the idempotency of the given object. Such an expectation is supported also by classical results in the theory of semigroups and rings. In a residually finite semigroup every element is divisible if and only if it is idempotent (see [17]). In particular, this is true also for a finitely generated commutative semigroup, as such a semigroup is residually finite by a well known theorem of Mal’cev

[82]. Similarly, in a finitely generated commutative ring the only divisible element is the zero element.

Finally, an interesting result was obtained for compact topological semirings with a unity [58]. It says that the set A of all additively divisible elements of such a semiring is non-empty, topologically closed and every element of A is additively idempotent.

All these results support the plausibility of the following conjectures. Let us recall that by $\mathcal{CF}$ we denote the class of all finitely generated commutative semirings.

Conjectures (Part I)

(1) Every infinite ideal-simple semiring $S \in \mathcal{CF}$ is idempotent or (additively) constant.

(1') Every parasemifield $S \in \mathcal{CF}$ is idempotent.

(2) No semiring $S \in \mathcal{CF}$ contains a copy of the semiring $\mathbb{Q}^+$.

(2') No semiring $S \in \mathcal{CF}$ with a unity contains a copy of the semiring $\mathbb{Q}^+$ that shares this unity.

(2") Every divisible semiring $S \in \mathcal{CF}$ with a unity is idempotent.

(3) Every uniquely divisible semiring $S \in \mathcal{CF}$ is idempotent.

(3') Every divisible semiring $S \in \mathcal{CF}$ is idempotent.

These conjectures are related in the following way.

Theorem 3.2.1. ([51, 64]) (3) $\Leftrightarrow$ (3') $\implies$ (2) $\Leftrightarrow$ (2') $\Leftrightarrow$ (2") $\implies$ (1) $\Leftrightarrow$ (1')

The equivalence of (1) and (1') was investigated in [53] and proved in [51]. In [64] we proved the rest of the implications and equivalences (in [64], Conjecture (1) is not cited in its right form, the additively constant case was omitted there). In [64] we also provided a basic characterization of the idempotency in terms of the divisibility (unique divisibility, resp.) in the commutative semirings.

Assigning properties (the divisibility or the idempotency) to a given structure (semigroup, ring, semiring) can be seen as a *global* approach. In this way our conjectures are formulated. On the other hand, we can also study these properties in a *point-wise* nature, i.e., we assign them to a given element $a \in S$ only. According to the known results mentioned above, divisibility implies idempotency for a single element in the case of semigroups or rings that are commutative and finitely generated. In view of these results we can ask the following question.

- To what extend is this behaviour (i.e., that the divisibility point-wisely implies the torsion) preserved or generalized in finitely generated commutative semirings?

We provide an answer in terms of free objects in the category of the commutative semirings (Section 3.3).

Finally, let us note that divisibility was investigated also for non-commutative structures. Divisible semigroups were studied in [13, 102], and as topological semigroups (in particular, the compact ones) they were investigated, e.g., in [6, 9, 10, 11, 12, 14, 29, 44]. Unlike the commutative case, there exist infinite but finitely generated divisible (non-commutative) groups (see [39] and [94]).

In rings, the problem whether a finitely generated *non-commutative* ring may contain the field $\mathbb{Q}$ seems to be still open. Nevertheless, in a related problem of finding an infinite division ring which is finitely generated as a ring [25, Problem 1.171], the first steps were recently made in [1].

3.3 Idempotency and divisibility in one-generated semirings

For the investigation of conjectures listed in Section 3.2, a natural approach is to start with semirings with one generator. It turns out that this case brings surprising results and that also the proofs are not straightforward.

In [54] it was proved that no non-trivial parasemifield is a one-generated semiring. This trivially confirms Conjecture (1') for such a case. In [71] we proved Conjectures (3') and (2") for one-generated semirings. In addition, Conjecture (3') was confirmed for the case of two generators where one of them was the unity. Our approach was based on rewriting the polynomials.

Theorem 3.3.1. ([71]) *Every one-generated divisible semiring is idempotent. Moreover, if the generator is multiplicatively invertible then the semiring is finite.*

Notice that in contrast to the case of parasemifields there do exist one-generated additively idempotent semifields [51].

Further, in [71] we have investigated embeddings of semigroups into the additive part of the finitely generated commutative semirings and we have obtained the following surprising result.

Theorem 3.3.2. ([71]) *Let $A(+)$ be an at most countable commutative semigroup, $n \in \mathbb{N}$, $a_1, \ldots, a_n \in A$ and $f \in \mathbb{N}[x_1, \ldots, x_n]$ be a non-constant polynomial.*

If either $n \geq 2$ or if f contains at least two different monomials, then there are a commutative semiring S and elements $w_1, \ldots, w_n \in S$ such that

(i) $S = \{g(w_1, \ldots, w_n) \mid g \in \mathbb{N}[x_1, \ldots, x_n]\}$,

(ii) *$A(+)$ is a subsemigroup of $S(+)$,*

(iii) $f(w_1, \ldots, w_n) = a_1$.

Moreover, if $n \geq 2$ and $f = x_1$ then S can be chosen such that $w_i = a_i$ for every $i = 1, \ldots, n-1$.

First, let us note that the proof of Theorem 3.3.2 works indeed for the *non-constant* polynomials (in [71] this condition was omitted). Constant polynomials $f = k \in \mathbb{N}$ are not covered by this theorem (in fact, they are assumed to have restrictions that follow from Conjectures (4) and (5) in the next Section 3.4).

Further, let us notice that if, in addition, f has no constant term then, according to the proof of Theorem 3.3.2, $A \subseteq \{g(w_1, \ldots, w_n) \,|\, g \in F(x_1, \ldots, x_n)\}$ and S might be in this case chosen to be a factor of the free commutative semiring $F(x_1, \ldots, x_n)$.

An immediate corollary is now the following.

Corollary 3.3.3. ([71]) *Every at most countable commutative semigroup is contained in the additive part of some one-generated semiring.*

This result shows that there is a significant difference between proper semirings and rings - finitely generated commutative rings cannot for instance contain the group $\mathbb{Q}(+)$ as a *subgroup* in their additive reducts, while semirings may do. On the other hand, our conjectures still suppose that the semiring $\mathbb{Q}^+(+,\cdot)$ cannot be contained as a *subsemiring* in any finitely generated commutative semiring.

The only case of a non-constant polynomial in Theorem 3.3.2 that remained uncovered was for $n = 1$ and the given polynomial has only one monomial. This situation that corresponds to a one-generated semiring was further investigated in [70] and has resulted into the following theorem.

Theorem 3.3.4. ([70]) *Let S be a semiring generated by an element $w \in S$. Then for $k, m \in \mathbb{N}$ and an element $z = kw^m \in S$ the following holds:*

- *z is divisible $\Leftrightarrow$ z is idempotent.*

Now we can provide the promised answer to the question from Section 3.2 in terms of the free commutative semirings $F(x_1, \ldots, x_n)$ (it follows from Theorems 3.3.2 and 3.3.4).

Theorem 3.3.5. *Let $n \in \mathbb{N}$. For $f \in F(x_1, \ldots, x_n)$ the following are equivalent:*

(i) For every semiring S and every semiring epimorphism $\varphi : F(x_1, \ldots, x_n) \to S$, the element $\varphi(f)$ is divisible if and only if $\varphi(f)$ is idempotent.

(ii) $n = 1$ and $f = k \cdot x_1^m$ for some $k, m \in \mathbb{N}$.

3.4 Conjectures related to torsion

Results concerning the connection between the idempotency and the divisibility motivated us to find a similar correspondence between the torsion (as a relaxed version of the idempotency) and some weaker version of the divisibility.

Within our investigating of the torsion, a special attention was paid to the case when a given element in a semiring S lies in some subgroup of the additive reduct of S. A semiring where every element has such a property is (additively) regular and, due to the commutativity of its additive reduct, it is also (additively) inverse. Regularity and inversion are classical properties studied in semigroups (see e.g. [38, 45, 76, 96]). They are natural generalizations of the notion of a group. Within the additive reducts of semirings these properties were investigated in more detail e.g., in [35, 59, 60, 97, 99, 106]. Here a more general notion of a semiring was assumed with a generally non-commutative additive reduct. To illustrate how these types of semirings are close to rings it is worth mentioning that recently [46] a characterization of additively regular semirings was provided - they are precisely those semirings (with a unity and a zero) where every semimodule has an injective envelope.

Based on these motivations for semirings from the class $\mathcal{CF}$ we have suggested notions of almost-divisibility (as a counterpart to the torsion) and strong almost-divisibility (as a counterpart to the torsion together with the regularity). Of course, both these new properties were chosen to be weaker than the original divisibility. The name of the second one is introduced in this thesis to make the reading simpler.

For a semiring S and a non-empty subset M of integers $\mathbb{N}$, let us call an element $a \in S$

- *M-divisible* $\Leftrightarrow$ for every $m \in M$ there is $c \in S$ such that $a = m \cdot c$.
- *almost-divisible* $\Leftrightarrow$ there is an infinite set P of prime numbers and $b \in \langle a \rangle^{+} = \mathbb{N} \cdot a$ such that b is P-divisible.
- *strongly almost-divisible* $\Leftrightarrow$ there is an infinite set P of prime numbers such that a is P-divisible.

Again, we assign such a notion to the semiring S itself if every element of S is so. For a subset $X \subseteq S$, let us still denote by $\left(\frac{X}{M}\right)_S = \{a \in S \,|\, (\exists x \in X)(\exists m \in M)\; x = ma\}$ the set of all possible fractions of all elements of X with respect to the set of "denominators" of M.

The following diagram shows the natural relations between all the properties that we consider. It is not difficult to check the validity of the implications.

$$\begin{tikzcd}
\text{idempotent} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{regular and torsion} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{torsion} \arrow[d, Rightarrow] \\
\text{divisible} \arrow[r, Rightarrow] & \text{strongly almost-divisible} \arrow[r, Rightarrow] & \text{almost-divisible.}
\end{tikzcd}$$

Now we may naturally ask whether the vertical implications can be reversed for a semiring $S \in \mathcal{CF}$. Based on these questions the following conjectures were suggested in [69] and [70].

Conjectures (Part II)([69, 70])

(4) Every strongly almost-divisible semiring $S \in \mathcal{CF}$ is regular and torsion.

(5) Every almost-divisible semiring $S \in \mathcal{CF}$ is torsion.

The previous and the new conjectures are related as follows.

$$(5) \implies (4) \implies (3)$$

Since the proof of these implications is not explicitly written in the attached papers, let us make a short explanation. The implication (4)⇒(3) follows immediately from the basic characterization of the additive idempotency in terms of the additive divisibility [64, 3.1.1]. To see the implication (5)⇒(4), one only needs to prove that for a torsion semiring $S \in \mathcal{CF}$ the strong almost-divisibility implies the regularity. By [64, 2.1], there is $k \in \mathbb{N}$ such that $kx = 2kx$ for every $x \in S$. Hence, by the basic properties of the cyclic semigroups, the set $G_x = \{\ell x \mid \ell \in \mathbb{N}, \ell \geq k\}$ is a finite additive group for every $x \in S$. Now, by the strong almost-divisibility, for every $a \in S$ there is a prime number $p \in \mathbb{N}$ big enough such that $a = px \in G_x$ for some $x \in S$. Thus the element a is contained in an additive group and the semiring S is therefore regular.

Similarly, as in Section 3.2, we may ask whether the remaining vertical implications in the diagram can be reversed for a *single* element $a \in S$ in a finitely generated commutative semiring S.

These questions as well as the new conjectures are again supported by results on the commutative semigroups and rings that we have shown in [69] and [70].

Theorem 3.4.1. ([69, 70])

(1) For a finitely generated commutative ring R and $a \in R$ the following holds:

- *a is almost-divisible ⇔ a is torsion.*

(2) For a residually finite commutative semigroup A (i.e., for A that is a subdirect product of finite commutative semigroups) and $a \in A$ the following holds:

- *a is regular and torsion ⇔ a is M-divisible for some infinite set $M \subseteq \mathbb{N}$;*
- *a is torsion ⇔ there is $b \in \mathbb{N}\cdot a$ such that b is M-divisible for some infinite set $M \subseteq \mathbb{N}$.*

Let us note that the validity of Theorem 3.4.1 can also be extended to non-commutative residually finite semigroups if the regularity of an element is substituted by a *complete* regularity of this element (to preserve the property that the element a generates a finite group).

3.5 Torsion and divisibility in one-generated semirings

In [69] we have investigated the relation between the torsion and the almost-divisibility in the finitely generated commutative semirings. In particular, we have studied the question when the almost-divisibility implies the torsion point-wisely in terms of the free objects. For reasons similar to Section 3.3 (by using Theorem 3.3.2 on the embedding of semigroups), the only case that needed to be investigated was the case of a semiring S with one generator $w \in S$. Within this semiring the only elements that were uncovered in Theorem 3.3.2 were elements of the form kw^m for $k, m \in \mathbb{N}$.

Further, in [70] we have studied an analogous problem that concerns the strong almost-divisibility. Our answers to both questions are similar to Theorem 3.3.5.

Theorem 3.5.1. ([69]) *Let $n \in \mathbb{N}$. For $f \in F(x_1, \dots, x_n)$ the following are equivalent:*

(i) For every semiring S and every semiring epimorphism $\varphi : F(x_1, \dots, x_n) \to S$, the element $\varphi(f)$ is almost-divisible if and only if $\varphi(f)$ is torsion.

(ii) $n = 1$ and $f = k \cdot x_1^m$ for some $k, m \in \mathbb{N}$.

Theorem 3.5.2. *Let $n \in \mathbb{N}$. For $f \in F(x_1, \dots, x_n)$ the following are equivalent:*

(i) For every semiring S and every semiring epimorphism $\varphi : F(x_1, \dots, x_n) \to S$, the element $\varphi(f)$ is strongly almost-divisible if and only if $\varphi(f)$ is torsion and regular .

(ii) $n = 1$ and $f = k \cdot x_1^m$ for some $k, m \in \mathbb{N}$.

Let us emphasize that Theorem 3.5.2 (that follows immediately from [70, 0.1] and Theorem 3.3.2) is not an easy consequence of Theorem 3.5.1. A non-trivial part in its proof is the case when for the given $k, m \in \mathbb{N}$ and $w \in S$ there are polynomials $f_p(x_1) \in F(x_1)$ (indexed by infinitely many prime numbers p) such that $kw^m = p \cdot f_p(w)$, the degrees of f_p are arbitrarily large and f_p contain monomials of degrees less than m.

An immediate consequence of Theorems 3.5.1 and 3.5.2 is a confirmation of Conjectures (4) and (5) for the one-generated case of semirings.

Theorem 3.5.3. ([69, 70]) *Every one-generated almost-divisible semiring is torsion. Every one-generated strongly almost-divisible semiring is torsion and regular.*

According to these results, equivalences between the (versions of) divisibility and the (versions of) torsion on the point-wise level may hold (in terms of the free objects) only for special elements in the one-generated semirings. For such a kind of an element $a \in S$ it is then natural to further investigate the set $\left(\frac{a}{\mathbb{N}}\right)_S$ of all its possible fractions in the semiring S. The following theorem in [70] gives a certain limitation.

Theorem 3.5.4. ([70]) *Let S be a semiring generated by $w \in S$. For every $m \in \mathbb{N}$ there is $k \in \mathbb{N}$ such that for the set $M = \{\ell \in \mathbb{N} \mid \gcd(\ell, k) = 1\}$ we have $\left(\frac{w^m}{M}\right)_S \subseteq \langle w, w^2, \ldots, w^m\rangle^+$. In particular, $\left(\frac{w}{M}\right)_S \subseteq \langle w\rangle^+$.*

This result can be interpreted in a way that "most" of the fractions of the element $a = w^m$ is concentrated in a "small" part of the semiring S (i.e., these fractions are contained in a finitely generated subsemigroup of $S(+)$). On the other hand, an example in [70, 0.5] shows that a similar property does not hold in general for the remaining elements $a = kw^m$, where $k \geq 2$.

To conclude this section, let us illustrate the behaviour of the set of fractions in the finitely generated commutative rings. Here we have obtained a stronger result [70].

Theorem 3.5.5. ([70]) *Let R be a finitely generated commutative ring and $G(+)$ be a finitely generated subgroup of $R(+)$. Then there is $k \in \mathbb{N}$ such that for the set $M = \{\ell \in \mathbb{N} \mid \gcd(\ell, k) = 1\}$ we have $\left(\frac{G}{M}\right)_R \subseteq G$.*

3.6 Commutative parasemifields

In this section we provide an answer to Conjecture (1') on parasemifields. Let us recall that a parasemifield is a semiring where the multiplicative semigroup is a group (for on overview, see e.g. [104]). Natural examples are the parasemifield of positive rationals $\mathbb{Q}^+$ or positive reals $\mathbb{R}^+$ (with standard operations) or parasemifields of all continuous positive real-valued functions on a topological space X equipped with the point-wise addition and multiplication. Let us recall that parasemifields are also essential structures in tropical geometry, they are used in representation theory for constructing cluster algebras [28] or appear in the process of so called dequantization [78].

Another type of examples of parasemifields arises through a natural duality with (abelian) lattice-ordered groups (ℓ-groups) that play an important rôle in algebra and related areas of mathematics, see e.g [68, 79, 101]. An (abelian) *ℓ-group* $G(\,\cdot\,,\ ^{-1}, 1, \wedge, \vee)$ is an algebraic structure such that $G(\,\cdot\,,\ ^{-1}, 1)$ is an abelian group, $G(\wedge, \vee)$ is a lattice and for all $a, b, c \in G$ it holds that $a(b \vee c)v = ab \vee ac$ and $a(b \wedge c) = ab \wedge ac$.

Such an ℓ-group is now term-equivalent to a commutative idempotent parasemifield $G(+, \cdot,\ ^{-1}, 1)$ with the correspondence of the operations given by $a \vee b = a + b$ and $a \wedge b = (a^{-1} + b^{-1})^{-1}$ for all $a, b \in G$.

An ℓ-group G (and the corresponding parasemifield) is called *unital* if there is an element $u \in G$ such that for every $x \in G$ there is $n \in \mathbb{N}$ with $x \leq u^n$. The class of all unital abelian ℓ-groups is categorically equivalent via the celebrated Mundici functor with the class of MV-algebras [90]. These provide a useful tool in studying the multi-valued logic of Łukasiewicz [5, 19, 20, 80, 91].

The equivalence between a commutative parasemifield S and its ℓ-group counterpart preserves finite generation in the sense that S is finitely generated as an ℓ-group if and only if S is finitely generated as a parasemifield. However, these cases are not equivalent to the property of being finitely generated as a semiring (i.e., when $S \in \mathcal{CF}$), which is generally stronger. In [52] it was noted that a commutative idempotent parasemifield $S \in \mathcal{CF}$ is unital as an ℓ-group. In [15] finitely generated unital (abelian) ℓ-groups were classified using the combinatorial notion of a stellar sequence, which is a sequence of certain simplicial complexes in $[0,1]^n \subseteq \mathbb{R}^n$. Based on this approach, in [52] idempotent parasemifields that are finitely generated as semirings were classified using the notion of a rooted tree.

As it was mentioned in Section 3.2, a conjecture was raised (Conjecture (1')) that every commutative parasemifield that is finitely generated as a semiring has to be idempotent. In [54] and [49] this conjecture was confirmed for the case of at most two generators.

Our result in [57] proves Conjectures (1) and (1') in the full generality and it is also a continuation of the study of idempotent parasemifields in [52].

Theorem 3.6.1. ([57]) *(a) Every commutative parasemifield that is finitely generated as a semiring is additively idempotent.*

(b) Every commutative proper semifield that is finitely generated as a semiring is either additively idempotent or additively constant.

(c) Every commutative proper finitely generated ideal-simple semiring is either additively idempotent or additively constant.

Let us recall that the latter theorem can also be understood as an extension of a theorem saying that every (commutative) field that is finitely generated as a ring has to be finite.

The key point for proofs in [57] was a careful study of convex cones associated to parasemifields. It turned out that they had a distinguished property called prismality (see [57] for more details). As a corollary, in [57] we obtained the following result.

Corollary 3.6.2. ([57]) *Let S be a commutative parasemifield that is finitely generated as a semiring. Then S is finitely generated as a multiplicative semigroup.*

Chapter 4

Congruence-simple semirings

4.1 Basic classification and cryptographical applications

In order to develop a structure theory for semirings, the congruence-simple semirings are one of the basic objects to study. They provide the simplest cases of subdirectly irreducible semirings that, according to the Birkhoff's theorem, are the basic buildings blocks in the variety of semirings. A deeper interest in the congruence-simple semirings started quite recently. These semirings are studied not only for their structural rôle but also because of their applications (see e.g. [23, 24, 26, 56, 61, 88, 89, 108]). It was shown (see e.g., [84]) that there are close connections between the public key cryptography based on the Discrete Logarithm Problem and the congruence-simple semirings and their semimodules. In particular, the use of the congruence-simple semirings is advantageous to avoid the Pohlig-Hellman type attacks, as the computation within such a semiring can not be simplified by any non-trivial semiring homomorphism.

Commutative congruence-simple semirings were successfully characterized and partially classified in [23] with an exception of the subsemirings of positive reals. Surprisingly, even the structure of subsemirings (and subsemigroups) of $\mathbb{Q}$ - a fairy basic object - is not well understood (in contrast to the structural properties of the subrings and subgroups of $\mathbb{Q}$ which are quite well known). A significant contribution to this problem was presented in [55, 56]. In this work all maximal subsemirings of the positive rational numbers were found and classified (with the help of prime p-adic valuations) and a similar problem for the congruence-simple ones was solved. Such a maximal congruence-simple subsemiring of $\mathbb{Q}^+$ is of the form $\{x \in \mathbb{Q}^+ \mid a^{v_p(x)} < x\}$, where $0 < a < 1$ is a real number and v_p is a valuation for a prime number p. These semirings are all non-isomorphic so there is uncountably many of them. As an open question it remains, whether or not the list of the congruence-simple subsemirings of $\mathbb{Q}^+$ found in [56] is already complete. These results were a part of author's dissertation.

A (generally non-commutative) congruence-simple semiring S with at least three elements fits into precisely one of the following four basic classes (see [24]):

- S is additively constant;
- S is additively cancellative (i.e., $a + c \neq b + c$ for all $a, b, c \in S$, $a \neq b$);
- S is additively nil of index 2 (i.e., there is $o \in S$ such that $2a = o$ for every $a \in S$) and $S = \{a + b \mid a, b \in S\}$;
- S is additively idempotent.

The first class consists of all multiplicative congruence-simple semigroups (with an absorbing element) that are equipped with a constant addition. Semirings in the second class can be embedded into rings, so this class includes all simple rings and many subsemirings of ordered rings. Examples of this type are for instance the semiring of all $n \times n$ matrices over positive rationals $\mathbb{Q}^+$ or the semiring of positive reals $\mathbb{R}^+$. The third class may contain only infinite non-commutative semirings [27]. An example of this type was constructed in [26] but the rest of this class remains enigmatic so far.

Finally, the fourth class can be viewed as congruence-simple semirings consisting of (some) endomorphisms of a given semilattice. Thanks to this natural interpretation, this class is of interest in the theory as well as it has a potential in the applications. Finite semirings of this type were used for a construction of the Diffie-Hellman type of cryptographical protocols ([84, 89]). Possible links of the infinite semirings to cryptography are not clear yet but this direction can be promising, especially in the case when the semirings satisfy some finiteness conditions.

To illustrate an application of semirings in the cryptography, let us provide the following two key-exchange protocols adapted from [22, 107]. Here two participants Alice and Bob want to agree on a common secret key k via an unsecured channel for their communication.

Protocol 1. Alice and Bob *publicly agree* on a proper congruence-simple semiring S and an element $u \in S$. Then:

1. Alice chooses a random element $\alpha \in S$ as *her secret key.* She computes $A = \alpha \cdot u$ as *her public key* and sends A to Bob.
2. Bob chooses a random element $\beta \in S$ as *his secret key.* He computes $B = u \cdot \beta$ as *his public key* and sends B to Alice.
3. Alice computes $k_A = \alpha \cdot B = \alpha \cdot (u \cdot \beta)$.
4. Bob computes $k_B = A \cdot \beta = (\alpha \cdot u) \cdot \beta$.

At the end of the protocol, both users obtain the same *common secret key* $k = k_A = k_B = \alpha \cdot u \cdot \beta$.

In order to break this protocol and find k (by knowing S, u, A and B only), it is sufficient to find an element $\alpha' \in S$ such that $\alpha' \cdot u = A$ (or solve the similar problem for B). Then $\alpha' \cdot B = (\alpha' \cdot u) \cdot \beta = A \cdot \beta = k$. This task seems to be difficult, as the multiplication in S is not invertible in general and we cannot use any non-trivial homomorphism on S to simplify the computation and gain in this way additional information.

In the second protocol we use the fact that for an element $u \in S$ and for two polynomials $f(x), g(x) \in F(x)$ with non-negative integer coefficients (and no constant terms) the elements $f(u) \in S$ and $g(u) \in S$ mutually commute in S.

Protocol 2. At the beginning both users Alice and Bob *publicly agree* on a proper congruence-simple semiring S and two elements $\alpha, \beta \in S$ that do not commute. Then:

1. Alice selects as *her secret key* two random polynomials $p_1(x), p_2(x) \in F(x)$. She computes *her public key* $A = p_1(\alpha) \cdot p_2(\beta)$ and sends A to Bob.

2. Bob selects as *his secret key* two random polynomials $q_1(x), q_2(x) \in F(x)$. He computes *his public key* $B = q_1(\alpha) \cdot q_2(\beta)$ and sends B to Alice.

3. Alice computes $k_A = p_1(\alpha) \cdot B \cdot p_2(\beta) = p_1(\alpha) \cdot \big(q_1(\alpha) \cdot q_2(\beta)\big) \cdot p_2(\beta)$.

4. Bob computes $k_B = q_1(\alpha) \cdot A \cdot q_2(\beta) = q_1(\alpha) \cdot \big(p_1(\alpha) \cdot p_2(\beta)\big) \cdot q_2(\beta)$.

At the end of the protocol, both users obtain the same *common secret key* $k = k_A = k_B$.

The problem on which the security of this protocol is based is as follows. To find the key k (by knowing S, α, β, A and B only) it is sufficient to find polynomials $p'_1(x), p'_2(x) \in F(x)$ such that $A = p'_1(\alpha) \cdot p'_2(\beta)$ (or solve the same problem for B). Then $p'_1(\alpha) \cdot B \cdot p'_2(\beta) = p'_1(\alpha) \cdot \big(q_1(\alpha) \cdot q_2(\beta)\big) \cdot p'_2(\beta) = q_1(\alpha) \cdot \big(p'_1(\alpha) \cdot p'_2(\beta)\big) \cdot q_2(\beta) = q_1(\alpha) \cdot A \cdot q_2(\beta) = k$.

Also, this task seems to be generally difficult for the reasons similar to the previous protocol.

4.2 Idempotent semirings with a bi-absorbing element

A fruitful approach for studying the congruence-simple additively idempotent semirings is to consider them as semirings of endomorphisms of their idempotent semimodules (i.e., of semilattices). The case when such an S-semimodule M has many endomorphisms coming from the semirings S is of special importance (see e.g.

[2, 3, 50, 63, 66]). By investigating such type of semimodules, the finite congruence-simple semirings were classified in [63, 108] up to an exceptional case of additively idempotent semirings with a bi-absorbing element. By extending similar ideas to generally infinite semirings we have studied a notion of an o-characteristic semimodule in [65].

To define this notion, let us first denote by $End_1(M)$, for a semilattice $M(+)$ with the greatest element $o_M \in M$ and with $|M| \geq 2$, the semiring of all endomorphisms of $M(+)$ that preserve the element o_M. Further, let $X_1(M)$ be the set of all such endomorphisms $\varphi \in End_1(M)$ with the range $\varphi(M) = \{o_M, u\}$ for some $u \in M \setminus \{o_M\}$ such that the downwards closed subsemilattice $\{x \in M \mid \varphi(x) \leq u\}$ has a greatest element. Now, a semilattice M with the greatest element $o_M \in M$ and with $|M| \geq 2$ is called an *o-characteristic S-semimodule* if it is equipped with an injective semiring homomorphism $\Phi : S \to End_1(M)$ such that $X_1(M) \subseteq \Phi(S)$.

In [65] we have shown a uniqueness of such a semimodule for the additively idempotent semirings with a bi-absorbing element.

Theorem 4.2.1. ([65]) *Let S be an additively idempotent semiring with a bi-absorbing element. If M is an o-characteristic S-semimodule, then S has at least one minimal left ideal and M is isomorphic to any such a minimal left ideal of S. Moreover, the semiring S then has at most one minimal left ideal I such that $x^2 = x$ for every $x \in I$.*

In mathematics there often appear semirings that have a zero element (i.e., the additively neutral and multiplicatively absorbing element). For additively idempotent semirings the zero element is the least element (with respect to the natural order), while, on the contrary, a bi-absorbing element is the greatest element. These two cases are essentially different (and disjoint for non-trivial semirings) and they cannot be transformed one to the other by simply turning the semiring "upside-down". A congruence-simple semiring with a zero is either a ring or it is additively idempotent [24].

Finite idempotent congruence-simple semirings with a zero were fully characterized in [108]. In [66] a similar characterization was generalized to some infinite cases. Finite idempotent congruence-simple semirings with a bi-absorbing element were studied in [63] and a subclass of such semirings that, in addition, have an additively neutral element was characterized by an existence of an irreducible idempotent semimodule (see [63] for the detailed definitions).

Our generalization of the characterization in [63] and also an analogy to the result in [66] now reads as follows.

Theorem 4.2.2. ([65]) *Let S be an additively idempotent semiring with a bi-absorbing element and with an additively neutral element. Assume further that $|S| \geq 3$ and*

- *every downwards closed subsemilattice K of $S(+)$ such that both the sets K and $S \setminus K$ are infinite has a greatest element.*

Then the following three conditions are equivalent:

(i) The semiring S is congruence-simple and has at least one minimal left ideal.

(ii) There is an o-characteristic S-semimodule M.

(iii) S is congruence-simple and there is a faithful minimal S-semimodule L.

To present our final result, let us denote by $\overline{X}_1(M)$, for a (non-trivial) semilattice M with a greatest element o_M, the set of all endomorphisms from $End_1(M)$ with the range of cardinality at most 2. Clearly, $X_1(M) \subseteq \overline{X}_1(M)$.

In [50] it was shown that a subsemiring S of $End_1(M)$ containing the set $\overline{X}_1(M)$ is congruence-simple if and only if for every $a \in S$ there is $e \in \overline{X}_1(M)$ such that $e \leq a$.

We have generalized this result in [65] by assuming that S contains, in comparison to [50], only the set $X_1(M)$ that is in general substantially smaller than $\overline{X}_1(M)$.

Theorem 4.2.3. ([65]) *Let M be a semilattice with a greatest element o_M and $|M| \geq 2$. Let S be a subsemiring of $End_1(M)$ such that $X_1(M) \subseteq S$. Then S has a bi-absorbing element and*

(i) the following two conditions are equivalent:

(α) S is congruence-simple,

(β) for every $a \in S$ there are $e \in X_1(M)$ and $b \in S$ such that $eb \leq a$.

(ii) the following two conditions are equivalent:

(γ) S is congruence-simple and for all $w \in M \setminus \{o_M\}$ and $a \in S$ the set $A = \{x \in M \mid ax \leq w\}$ is upwards bounded in $M \setminus \{o_M\}$ (provided that A is non-empty),

(δ) for every $a \in S$ there is $e \in X_1(M)$ such that $e \leq a$.

Bibliography

[1] A. Atkarskaya, A. Kanel-Belov, E. Plotkin, E. Rips, *Construction of a quotient ring of $\mathbb{Z}_2\mathcal{F}$ in which a binomial $1 + w$ is invertible using small cancellation methods*, in: E. Plotkin (Ed.), Groups, Algebras and Identities, Contemp. Math. **726**, Amer. Math. Soc., 2019, pp. 1–76.

[2] B. Batíková, T. Kepka, P. Němec, *Characteristic semimodules*, Ital. J. Pure Appl. Math. **37** (2017), 361–376.

[3] B. Batíková, T. Kepka, P. Němec, *Critical semimodules*, Ital. J. Pure Appl. Math. **38** (2017), 172–183.

[4] T. Beke, *The Grothendieck ring of varieties and of the theory of algebraically closed fields*, J. Pure Appl. Algebra **221(2)** (2017), 393–400.

[5] L. P. Belluce, A. Di Nola, A. R. Ferraioli, *Ideals of MV-semirings and MV-algebras*, in: G. L. Litvinov, S. N. Segreev (Eds.), Tropical and Idempotent Mathematics and Applications: International Workshop, Contemp. Math. **616**, Amer. Math. Soc., 2014, pp. 59–76.

[6] K. Benningfield, *Cancellation and embedding theorems for compact uniquely divisible semigroups*, Semigroup Forum **58** (1999), 336–347.

[7] J. A. Bergstra, I. Bethke, A. Ponse, *Process algebra with combinators*, in: E. Börger, Yu. Gurevich, K. Meinke (Eds.), Computer Science Logic CSL '93, Lecture Notes in Comput. Sci. **832**, Springer, Berlin, 1994, pp. 36–65.

[8] S. Bistarelli, *Semirings for Soft Constraint Solving and Programming*, Lecture Notes in Comput. Sci. **2962**, Springer, 2004.

[9] D. R. Brown, M. Friedberg, *Representation theorems for uniquely divisible semigroups*, Duke Math. J. **35(2)** (1968), 341–352.

[10] D. R. Brown, M. Friedberg, *A survey of compact divisible commutative semigroups*, Semigroup Forum **1** (1970), 143–161.

[11] D. R. Brown, M. Friedberg, *Linear representations of certain compact semigroups*, Trans. Amer. Math. Soc. **160** (1971), 453–465.

[12] D. R. Brown, J. A. Hildebrant, *Embedding compact t-semigroups into compact uniquely divisible semigroups*, Semigroup Forum **41** (1990), 61–82.

[13] D. R. Brown, J. G. LaTorre, *A characterization of uniquely divisible commutative semigroups*, Pacific J. Math. **18(1)** (1966), 57–60.

[14] D. R. Brown, J. W. Stepp, *The structure semilattice of a compact UDC semigroup*, Semigroup Forum **31** (1985), 235–250.

[15] M. Busaniche, L. Cabrer, D. Mundici, *Confluence and combinatorics in finitely generated unital lattice-ordered abelian groups*, Forum Math. **24** (2012), 253–271.

[16] R. Castano-Bernard, et al (Eds.), *Homological Mirror Symmetry and Tropical Geometry*, Lect. Notes Unione Mat. Ital. **15**, Springer, Heidelberg, 2014.

[17] W. E. Clark, W. C. Holland, G. J. Székely, *Decompositions in discrete semigroups*, Studia Sci. Math. Hungar. **34** (1998), 15–23.

[18] R. Dedekind, *Über die Theorie der ganzen algebraischen Zahlen*, Supplement XI, in: P. G. L. Dirichlet (Ed.), Vorlesungen über Zahlentheorie, 4te Aufl., Friedrich Vieweg und Sohn, Braunschweig, 1894, pp. 434–627.

[19] A. Di Nola, B. Gerla, *Algebras of Łukasiewicz's logic and their semiring reducts*, in: G. L. Litvinov, V. P. Maslov (Eds.), Idempotent Mathematics and Mathematical Physics: International Workshop, Contemp. Math. **377**, Amer. Math. Soc., 2005, pp. 131–144.

[20] A. Di Nola, C. Russo, *The semiring-theoretic approach to MV-algebras: A survey*, Fuzzy Sets and Systems **281** (2015), 134–154.

[21] M. Droste, W. Kuich, H. Vogler (Eds.), *Handbook of Weighted Automata*, Monogr. Theor. Comput. Sci., Springer, 2009.

[22] M. Durcheva, *Semirings as Building Blocks in Cryptography*, Cambridge Scholars Publishing, 2020.

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

[24] R. El Bashir, T. Kepka, *Congruence-simple semirings*, Semigroup Forum **75** (2007), 588–608.

[25] V. T. Filippov, V. K. Kharchenko, I. P. Shestakov (Eds.), *The Dniester Notebook: Unsolved Problems in the Theory of Rings and Modules*, 4th ed., Inst. Math., Novosibirsk, 1993.

[26] V. Flaška, *One very particular example of a congruence-simple semiring*, Europ. J. Comb. **30(4)** (2009), 759–763.

[27] V. Flaška, T. Kepka, J. Šaroch, *Bi-ideal-simple semirings*, Comment. Math. Univ. Carolinae **46(3)** (2005), 391–397.

[28] S. Fomin, A. Zelevinsky, *Cluster algebras IV: Coefficients*, Compositio Math. **143** (2007), 112–164.

[29] M. Friedberg, *Homomorphisms of divisible semigroups*, Math. Z. **123** (1971), 215–218.

[30] A. Gathmann, *Tropical algebraic geometry*, Jahresber. Deutsch. Math. Verein. **108(1)** (2006), 3–32.

[31] S. Gaubert, MAX PLUS, *Methods and applications of* $(\max,+)$ *linear algebra*, in: R. Reischuk, M. Morvan (Eds.), STACS 97, Lecture Notes in Comput. Sci. **1200**, Springer, 1997, pp. 261–282.

[32] K. Głazek, *A Guide to the Literature on Semirings and their Applications in Mathematics and Information Sciences: With Complete Bibliography*, Kluwer Academic Publishers, Dordrecht, 2002.

[33] J. S. Golan, *The Theory of Semirings, with Applications in Mathematics and Theoretical Computer Science*, Pitman Monogr. Surv. Pure Appl. Math. **54**, Longman Scientific and Tech., Essex, 1992.

[34] J. S. Golan, *Power Algebras over Semirings: With Applications in Mathematics and Computer Science*, Math. Appl. **488**, Kluwer Academic Publishers, Dordrecht, 1999.

[35] J. S. Golan, *Semirings and their Applications*, Kluwer Academic Publishers, Dordrecht, 1999.

[36] J. S. Golan, *Semirings and Affine Equations over Them: Theory and Applications*, Math. Appl. **488**, Kluwer Academic Publishers, Dordrecht, 2003.

[37] M. Gondran, M. Minoux, *Graphs, Dioids and Semirings: New Models and Algorithms*, Oper. Res./Comput. Sci. Interfaces Ser. **41**, Springer, 2008.

[38] P. A. Grillet, *Semigroups: An Introduction to the Structure Theory*, Monogr. Textb. Pure Appl. Math. **193**, Marcel Dekker, New York, 1995.

[39] V. S. Guba, *A finitely generated complete group*, Izv. Akad. Nauk SSSR, Ser. Mat. **50(5)** (1986), 883–924 (in Russian) (English translation: Math. USSR Izv. **29(2)** (1987), 233–277).

[40] S. M. Gusein-Zade, I. Luengo, A. Melle-Hernández, *Power structure over the Grothendieck ring of varieties and generating series of Hilbert schemes of points*, Michigan Math. J. **54(2)** (2006), 353–359.

[41] F. Halter-Koch, *Ideal Systems: An Introduction to Multiplicative Ideal Theory*, Monogr. Textb. Pure Appl. Math. **211**, Marcel Dekker, Inc., New York, 1998.

[42] U. Hebisch, H. J. Weinert, *Semirings: Algebraic Theory and Applications in Computer Science*, Ser. Algebra **5**, World Scientific, Singapore, 1998.

[43] D. Hilbert, *Über den Zahlbegriff*, Jahresber. Deutsch. Math. Verein **8** (1900), 180–184.

[44] J. A. Hildebrant, *On compact divisible abelian semigroups*, Proc. Amer. Math. Soc. **19(2)** (1968), 405–410.

[45] J. H. Howie, *Fundamentals of Semigroup Theory*, London Math. Soc. Monogr. **12**, Clarendon Press, Oxford, 1995.

[46] S. N. Il'in, *On semirings all of whose semimodules have injective envelopes*, J. Alg. Appl. **20(7)** (2021), 2150130, 12 pp.

[47] I. Itenberg, G. Mikhalkin, E. Shustin, *Tropical Algebraic Geometry*, 2nd ed., Oberwolfach Semin. **35**, Birkhäuser, Basel, 2009.

[48] Z. Izhakian, L. Rowen, *Supertropical algebra*, Adv. Math. **225(4)** (2010), 2222–2286.

[49] J. Ježek, V. Kala, T. Kepka, *Finitely generated algebraic structures with various divisibility conditions*, Forum Math. **24(2)** (2012), 379–397.

[50] J. Ježek, T. Kepka, *The semiring of 1-preserving endomorphisms of a semilattice*, Czech. Math. J. **59** (2009), 999–1003.

[51] J. Ježek, T. Kepka, *Finitely generated commutative division semirings*, Acta Univ. Carolin. Math. Phys. **51(1)** (2010), 3–27.

[52] V. Kala, *Lattice-ordered groups finitely generated as semirings*, J. Commut. Algebra **9(3)** (2017), 387–412.

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

[54] V. Kala, T. Kepka, M. Korbelář, *Notes on commutative parasemifields*, Acta Univ. Carol. Math. Phys. **50(4)** (2009), 521–533.

[55] V. Kala, T. Kepka, M. Korbelář, J. D. Phillips, *Various subsemirings of the field $\mathbb{Q}$ of rational numbers*, Acta Univ. Carol. Math. Phys. **50(1)** (2009), 29–59.

[56] V. Kala, M. Korbelář, *Congruence-simple subsemirings of* $\mathbb{Q}^+$, Semigroup Forum **81(2)** (2010), 286–296.

[57] V. Kala, M. Korbelář, *Idempotence of finitely generated commutative semifields*, Forum Math. **30(6)** (2018), 1461–1474.

[58] P. H. Karvellas, *Additive divisibility in compact topological semirings*, Canad. J. Math. **26(3)** (1974), 593–599.

[59] P. H. Karvellas, *Inverse semirings*, J. Aust. Math. Soc. **18(3)** (1974), 277–288.

[60] Y. Katsov, *Tensor products and injective envelopes of semimodules over additively regular semirings*, Algebra Colloq. **4(2)** (1997), 121–131.

[61] Y. Katsov, T. G. Nam, J. Zumbrägel, *On simpleness of semirings and complete semirings*, J. Algebra Appl. **13(6)** (2014), 1450015, 29 pp.

[62] B. Keller, *Cluster algebras and derived categories*, in: Y. Kawamata (Ed.), Derived Categories in Algebraic Geometry: Tokyo 2011, EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich, 2012, pp. 123–183.

[63] A. Kendziorra, J. Zumbrägel, *Finite simple additively idempotent semirings*, J. Algebra **388** (2013), 43–64.

[64] T. Kepka, M. Korbelář, *Conjectures on additively divisible commutative semirings*, Math. Slovaca **66(5)** (2016), 1059–1064.

[65] T. Kepka, M. Korbelář, P. Němec, *Simple semirings with a bi-absorbing element*, Semigroup Forum **101(2)** (2020), 406–420.

[66] T. Kepka, J. Kortelainen, P. Němec, *Simple semirings with zero*, J. Alg. Appl. **15(3)** (2016), 1650047, 9 pp.

[67] V. N. Kolokoltsov, V. P. Maslov, *Idempotent Analysis and Its Applications*, Math. Appl. **401**, Springer, 1997.

[68] V. M. Kopytov, N. Ya. Medvedev, *The Theory of Lattice-Ordered Groups*, Math. Appl. **307**, Springer, 1994.

[69] M. Korbelář, *Torsion and divisibility in finitely generated commutative semirings*, Semigroup Forum **95(2)** (2017), 293–302.

[70] M. Korbelář, *Divisibility and groups in one-generated semirings*, J. Algebra Appl. **17(4)** (2018), 1850071, 10 pp.

[71] M. Korbelář, G. Landsmann, *One-generated semirings and additive divisibility*, J. Algebra Appl. **16(2)** (2017), 1750038, 22 pp.

[72] W. Krull, *Axiomatische Begründung der allgemeine Idealtheorie*, Sitzungber. Phys.-Med. Soz. Erlangen **56** (1924), 47–63.

[73] W. Kuich, *Semirings, automata and combinatorial applications*, in: G. Baron, P. Kirschenhofer (Eds.), Act. Sém. Lothar. Combin., Publication de I.M.R.A. **358/5-18**, Strasbourg, 1988, pp. 5–51.

[74] W. Kuich, *Semirings and formal power series: Their relevance to formal languages and automata*, in: G. Rozenberg, A. Salomaa (Eds.), Handbook of Formal Languages, Vol. 1, Springer, Berlin, 1997, pp. 609–677.

[75] W. Kuich, A. Salomaa, *Semirings, Automata, Languages*, Monogr. Theoret. Comput. Sci. **5**, Springer, 1986.

[76] M. V. Lawson, *Inverse Semigroups: The Theory of Partial Symmetries*, World Scientific, Singapore, 1998.

[77] E. Leichtnam, *A classification of the commutative Banach perfect semi-fields of characteristic 1. Applications*, Math. Ann. **369** (2017), 653–703.

[78] G. L. Litvinov, *Maslov dequantization, idempotent and tropical mathematics: A brief introduction*, J. Math. Sci. **140(3)** (2007), 426–444.

[79] W. A. Luxemburg, A. C. Zaanen, *Riesz Spaces, Vol. 1*, North Holland, Amsterdam, 1971.

[80] F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press, Cambridge, 1916.

[81] D. Maclagan, B. Sturmfels, *Introduction to Algebraic Geometry*, Grad. Stud. Math. **161**, Amer. Math. Soc., Providence, 2015.

[82] A. I. Mal'cev, *On homomorphisms into finite groups*, Lecture Notes of Ivanovsk Pedagog. Inst. **18** (1958), 49–60 (in Russian) (English translation: L. J. Leifman (Ed.), Twelve Papers in Algebra, Amer. Math. Soc., 1983, pp. 67–79).

[83] M. Marshall, *Positive Polynomials and Sums of Squares*, Math. Surveys Monogr. **146**, Amer. Math. Soc., 2008.

[84] G. Maze, C. Monico, J. Rosenthal, *Public key cryptography based on semigroup actions*, Adv. Math. Commun. **1(4)** (2007), 489–507.

[85] W. M. McEneaney, *Max-plus Methods for Nonlinear Control and Estimation*, Systems Control Found. Appl., Birkhäuser, Basel, 2006.

[86] G. Mikhalkin, *Enumerative tropical algebraic geometry in* $\mathbb{R}^2$, J. Amer. Math. Soc., **18(2)** (2005), 313–377.

[87] M. Minoux, *Solving combinatorial problems with combined min-max - min-sum objective and applications*, Math. Program. (Ser. B) **45** (1989), 361–372.

[88] S. S. Mitchell. P. B. Fenoglio, *Congruence-free commutative semirings*, Semigroup Forum **37** (1988), 79–91.

[89] C. Monico, *On finite congruence-simple semirings*, J. Algebra **271(2)** (2004), 846–854.

[90] D. Mundici, *Mapping abelian l-groups with strong unit one-one into MV-algebras*, J. Algebra **98(1)** (1986), 76–81.

[91] D. Mundici, *Advanced Łukasiewicz Calculus and MV-algebras*, Trends Log. **35**, Springer, 2011.

[92] T. Nakanishi, *Tropicalization method in cluster algebras*, in: C. Athorne, D. Maclagan, I. Strachan (Eds.), Tropical Geometry and Integrable Systems, Contemp. Math. **580**, Amer. Math. Soc., 2012, pp. 95–116 .

[93] E. Nöther, *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörper*, Math. Ann. **96(1)** (1927), 26–61.

[94] A. Yu. Ol'shanskii, *Geometry of Defining Relations in Groups*, Math. Appl. **70**, Kluwer Academic Publishers, Dordrecht, 1991.

[95] L. Pachter, B. Sturmfels, *Algebraic Statistics for Computational Biology*, Cambridge University Press, 2005.

[96] M. Petrich, N. R. Reilly, *Completely Regular Semigroups*, Can. Math. Soc. Ser. Monogr. Adv. Texts **23**, Wiley, 1999.

[97] B. Pondělíček, *Inverse semirings whose additive endomorphisms are multiplicative*, Math. Slovaca **46(5)** (1996), 525–529.

[98] E. Shustin, Z. Izhakian, *A tropical Nullstellensatz*, Proc. Amer. Math. Soc. **135(12)** (2007), 3815–3821.

[99] O. Sokratova, *On semimodules over commutative, additively idempotent semirings*, Semigroup Forum **64** (2001), 1–11.

[100] D. Speyer, B. Sturmfels, *The tropical Grassmannian*, Adv. Geom. **4** (2004), 389–411.

[101] S. A. Steinberg, *Lattice-ordered Rings and Modules*, Springer, 2010.

[102] T. Tamura, *Minimal commutative divisible semigroups*, Bull. Amer. Math. Soc. **69(5)** (1963), 713–716.

[103] K. Thas (Ed.), *Absolute Arithmetic and* $\mathbb{F}_1$*-Geometry*, Eur. Math. Soc., 2016.

[104] E. M. Vechtomov, A. V. Cheraneva, *Semifields and their properties*, J. Math. Sci. (N. Y.) **163(6)** (2009), 625–661.

[105] H. J. Weinert, R. Wiegandt, *On the structure of semifields and lattice-ordered groups*, Period. Math. Hung. **32(1-2)** (1996), 129–147.

[106] J. Zeleznikow, *Regular semirings*, Semigroup Forum **23** (1981), 119–136.

[107] J. Zumbrägel, *Public-key Cryptography Based on Simple Semirings*, dissertation, Zürich, 2008, 109 pp.

[108] J. Zumbrägel, *Classification of finite congruence-simple semirings with zero*, J. Algebra Appl. **7(3)** (2008), 363–377.

Appendix A

Attached publications

The following publications are included (listed in the order they appear in this thesis):

- T. Kepka, M. Korbelář, *Conjectures on additively divisible commutative semirings*, Math. Slovaca **66(5)** (2016), 1059–1064.
- M. Korbelář, G. Landsmann, *One-generated semirings and additive divisibility*, J. Algebra Appl. **16(2)** (2017), 1750038, 22 pp.
- M. Korbelář, *Torsion and divisibility in finitely generated commutative semirings*, Semigroup Forum **95(2)** (2017), 293–302.
- M. Korbelář, *Divisibility and groups in one-generated semirings*, J. Algebra Appl. **17(4)** (2018), 1850071, 10 pp.
- V. Kala, M. Korbelář, *Idempotence of finitely generated commutative semifields*, Forum Math. **30(6)** (2018), 1461–1474.
- T. Kepka, M. Korbelář, P. Němec, *Simple semirings with a bi-absorbing element*, Semigroup Forum **101(2)** (2020), 406–420.

DE GRUYTER

Mathematica Slovaca

DOI: 10.1515/ms-2016-0203
Math. Slovaca **66** (2016), No. 5, 1059–1064

CONJECTURES ON ADDITIVELY DIVISIBLE COMMUTATIVE SEMIRINGS

Tomáš Kepka* — Miroslav Korbelář**

(*Communicated by Miroslav Ploščica*)

ABSTRACT. We present a series of open questions about finitely generated commutative semirings with divisible additive semigroup. In this context we show that a finitely generated additively divisible commutative semiring is idempotent, provided that it is torsion. In the particular case of a one-generated additively divisible semiring without unit, such a semiring must contain an ideal of idempotent elements.

It is well known that a commutative field is finite provided that it is a finitely generated ring. Consequently, no finitely generated commutative ring (whether unitary or not) contains a copy of the field $\mathbb{Q}$ of rational numbers. On the other hand, it seems to be an open problem whether a finitely generated (commutative) semiring S can contain a copy of the semiring (parasemifield) $\mathbb{Q}^+$ of positive rationals. Anyway, if S were such a (unitary) semiring with $1_S = 1_{\mathbb{Q}^+}$, then the additive semigroup $S(+)$ should be divisible. So far, all known examples of finitely generated additively divisible commutative semirings are additively idempotent. Hence a natural question arises, whether a finitely generated (commutative) semiring with the divisible additive part has to be additively idempotent (see 1.1(A)).

Analogous questions were studied for semigroups. According to [9: 2.5(iii)], there is a finitely generated non-commutative semigroup with a divisible element that is not idempotent. Moreover, there exists infinite but finitely generated divisible (non-commutative) group (see [12] and [19]). (Uniquely) divisible semigroups were studied in [7, 20] and as topological semigroups, especially the compact case, in [3–6, 8, 10, 11, 13] and recently in [2]. The property of additive divisibility in compact topological semiring was investigated in [17].

The present short note initiates a study of additively divisible commutative semirings together with a series of open questions about the finitely generated cases (see 1.1).

1. Conjectures

Throughout the rest of the paper, all algebraic structures involved (as semigroups, semirings, groups and rings) are assumed to be commutative, but, possibly, without additively and/or multiplicatively neutral elements. Consequently, a *semiring* is a non-empty set equipped with two commutative and associative binary operations, an addition and a multiplication, such that the multiplication distributes over the addition. A semiring S is called a *ring* iff the additive semigroup of S is a group and S is called a *parasemifield* iff the multiplicative semigroup of S is a non-trivial group. We denote by $1_S \in S$ the fact that S has a multiplicative unit 1_S (in the opposite case we write $1_S \notin S$).

2010 Mathematics Subject Classification: Primary 12K10, 16Y60, 20M14.
Keywords: commutative semiring, divisible semigroup, idempotent, torsion.
The second author was supported by the project LC 505 of Eduard Čech's Center for Algebra and Geometry.

We will use the usual notation: $\mathbb{N}$ for the semiring of positive integers and $\mathbb{Q}^+$ for the parasemifield of positive rationals.

Let $A(+)$ be a semigroup. An element $a \in A$ is called *divisible* (*uniquely divisible*, resp.) iff for every $n \in \mathbb{N}$ there exists $b \in A$ (a unique, resp.) such that $a = nb$. A semigroup is called *divisible* (*uniquely divisible*, resp.) if every its element is divisible (uniquely divisible, resp.). Clearly, A is divisible iff $A = nA$ for every $n \in \mathbb{N}$. The class of divisible semigroups is closed under taking homomorphic images and cartesian products and contains all divisible groups and all semilattices (i.e., idempotent semigroups).

Let S be a semiring. For an element $a \in S$ denote $\mathrm{ord}(a) := \mathrm{card}(\{ka \mid k \in \mathbb{N}\}) \in \mathbb{N} \cup \{\infty\}$ *the order of* a. For a subset $\emptyset \neq X \subseteq S$ put $\langle X\rangle$ the subsemiring of S generated by X. A semiring is called *additively divisible* (*additively uniquely divisible*, resp.) iff its additive part is a divisible semigroup (uniquely divisible semigroup, resp.). A commutative semigroup $M(+)$ is called an S*-semimodule* iff there is a semiring homomorphisms $\varphi\colon S \to \mathrm{End}(M(+))$. In the case when $1_S \in S$ and $\varphi(1_S) = \mathrm{id}_S$, the S-semimodule M is called *unitary.* Let $\mathcal{D}(S)$ denote the semiring extending S where a multiplicative unit is added freely. Now S can naturally be treated as a unitary $\mathcal{D}(S)$-semimodule.

***Examples* 1.**

(i) The semiring $\mathbb{Q}^+$ is additively (uniquely) divisible.

The zero-multiplication ring defined on the Prüfer group $\mathbb{Z}_{p^\infty}$ is both additively divisible and additively torsion. Of course, the ring is neither additively idempotent nor finitely generated. The (semi)group $\mathbb{Z}_{p^\infty}(+)$ is not uniquely divisible.

Consider a non-trivial semilattice L. Then the product $L \times \mathbb{Z}_{p^\infty}$ is a torsion divisible semigroup that is neither a semilattice nor a group.

(ii) Let R be a (non-zero) finitely generated ring (not necessary with unit). Then R has at least one maximal ideal I and the factor-ring R/I is a finitely generated simple ring. However, any such a ring is finite and consequently, R is not additively divisible.

Conjectures 1.1. Consider the following statements:

(A) Every finitely generated additively divisible semiring is additively idempotent.

(A1) Every finitely generated additively uniquely divisible semiring is additively idempotent.

(B) No finitely generated semiring contains a copy of $\mathbb{Q}^+$.

(B1) No finitely generated semiring with a unit element contains a copy of $\mathbb{Q}^+$ sharing the unit.

(B2) Every finitely generated additively divisible semiring with a unit is additively idempotent.

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

(C1) Every infinite finitely generated ideal-simple semiring is additively idempotent. (A semirings is called *ideal-simple* iff every its proper ideal is trivial. For further details see [1].)

Proposition 1.1. (A) $\iff$ (A1) $\implies$ (B) $\iff$ (B1) $\iff$ (B2) $\implies$ (C) $\iff$ (C1).

The proof of 1.1 follows in the last section 5. The conjecture (C) (with the equivalent version (C1)) was stated in [15] and was confirmed for the one-generated case in [16] and for the two-generated case in [14]. The other conjectures are supported by further study in this paper (especially by 3.1, 3.2, 3.2.3, 4.2, 4.1 and 2).

2. Preliminaries

Lemma 2.1. *Let $\emptyset \neq X$ be a subset of a semiring such that $m = \sup\{\mathrm{ord}(a) \mid a \in X\} \in \mathbb{N}$. Then $\sup\{\mathrm{ord}(b) \mid b \in \langle X\rangle\} < \infty$. Moreover, there is $r \in \mathbb{N}$ such that $2rb = rb$ for every $b \in \langle X\rangle$.*

Proof. For every $a \in X$ there are $k, t \in \mathbb{N}$ such that $ka = (k+t)a$ and $k+t \leq m+1$. Furthermore, $2\ell a = \ell a$ for some $\ell \in \mathbb{N}$, $\ell \leq m+1$. Setting $r = (m+1)!$, we get $2ra = ra$ for every $a \in X$. Hence $\mathrm{ord}(b) \leq 2r-1$ for every $b \in \langle X\rangle$. □

Lemma 2.2. *Let S be a semiring. Let $a, b \in S$ be such that $ka = la + b$ for some $k, l \in \mathbb{N}$, $k \neq l$. If* $\operatorname{ord}(b)$ *is finite, then* $\operatorname{ord}(a)$ *is so.*

Proof. There are $m, n \in \mathbb{N}$ such that $m < n$ and $mb = nb$. Then $nka = nla + nb = nla + mb = (n-m)la + m(la + b) = (n-m)la + mka = ((n-m)l + mk)a$. Since $k \neq l$, we see that $(n-m)k \neq (n-m)l$ and $nk \neq (n-m)l + mk$. Consequently, $\operatorname{ord}(a)$ is finite. □

Lemma 2.3. *Let S be a semiring. If $w \in S$, $a, b, c \in \mathcal{D}(S)w$ and $m \in \mathbb{N}$ are such that $ma = mb$ and $mc = w$, then $a = b$.*

Proof. For every $d \in \mathcal{D}(S)w$, there is $\alpha_d \in \mathcal{D}(S)$ with $d = \alpha_d w$. Now, $a = \alpha_a w = \alpha_a mc = \alpha_c \alpha_a mw = \alpha_c ma = \alpha_c mb = \alpha_c \alpha_b mw = \alpha_b mc = \alpha_b w = b$. □

Remark 1. Let S be a semiring and $x, v \in S$ be such that $x = 2x + v$. Put $\omega_x = x + v$. Then ω_x is an idempotent, $x = x + \omega_x$ and the set $\{b \in S \mid x = x + b\}$ is a subsemigroup of $S(+)$ with ω_x as an (uniquely determined) absorbing element.

3. Additively divisible semirings

Theorem 3.1. ([9: 2.5(i)]) *A divisible element in a finitely generated commutative semigroup is idempotent. In particular, a commutative semigroup is finitely generated and divisible if and only if it is a finite semilattice.*

Proposition 3.1.1. *The following are equivalent for a commutative semiring S:*

(i) *S is additively idempotent.*

(ii) *S is additively divisible and bounded* (*i.e.* $\sup\{\operatorname{ord}(a) \mid a \in S\} < \infty$).

(iii) *S is additively uniquely divisible and torsion.*

Proof. First, (i) $\Longrightarrow$ (ii) and (i) $\Longrightarrow$ (iii) are easy.

(ii) $\Longrightarrow$ (i): By 2.1 there exists $n \in \mathbb{N}$ such that $2na = na$ for every $a \in S$. Since S is divisible, we have $a = nb$, and so $2a = 2nb = nb = a$.

(iii) $\Longrightarrow$ (i): Since S is torsion, for every $a \in S$ there is $k \in \mathbb{N}$ such that $2ka = ka$. Now, S is additively uniquely divisible, hence $k(2a) = ka$ and $2a = a$. □

Theorem 3.2. *A finitely generated additively divisible semiring S is additively idempotent, provided that it is torsion.*

Proof. Follows immediately from 2.1 and 3.1.1. □

To verify the following two statements is an easy exercise.

Proposition 3.2.1. *A semiring S is uniquely additively divisible if and only if it is a unitary $\mathbb{Q}^+$-semimodule. In this case the structure of the $\mathbb{Q}^+$-semimodule is unique and provides a structure of the $\mathbb{Q}^+$-semialgebra* (*i.e.* $qa \cdot b = a \cdot qb$ *for all* $q \in \mathbb{Q}^+$ *and* $a, b \in S$).

Proposition 3.2.2. *Let S be an additively divisible semiring with a unit $1_S \in S$. Then S is additively uniquely divisible and either S is additively idempotent or it contains a subsemiring Q such that $Q \cong \mathbb{Q}^+$ and $1_S = 1_Q$.*

Proposition 3.2.3. *Let S be a non-trivial additively divisible semiring. Then S is not finitely generated, provided that it is additively cancellative.*

Proof. The difference ring $R = S - S$ of S is additively divisible, and hence it is not finitely generated by 1(ii). Then S is not finitely generated either. □

On a semiring S define a relation $\sigma_S = \{(a, b) \in S \times S \mid (\exists m \in \mathbb{N})[ma = mb]\}$. Clearly, σ_S is a congruence of S and $\sigma_{S/\sigma_S} = \mathrm{id}$. The following assertion is easy to verify (by 3.1.1).

Proposition 3.2.4.

(i) *A semiring S is torsion if and only if the factor-semiring S/σ_S is torsion.*

(ii) *Let S be an additively divisible semiring. Then the factor-semiring S/σ_S is additively uniquely divisible. If, moreover, S is torsion, then σ_S is just the smallest congruence of S such that the corresponding factor-semiring is additively idempotent.*

4. One-generated additively divisible semirings

In this section, let S be an additively divisible semiring generated by a single element $w \in S$. Further, let x be a variable and $F(x)$ denotes the free commutative semiring with the basis $\{x\}$ (i.e. $F(x)$ consists of just all non-zero polynomials over x with non-negative integer coefficients and with zero constant terms).

Proposition 4.1. *The semiring S is additively uniquely divisible.*

Proof. Follows from 2.3. □

Proposition 4.2. *The semiring S is additively idempotent, provided that* $\operatorname{ord}(w^m)$ *is finite for some $m \in \mathbb{N}$.*

Proof. Let $n \in \mathbb{N}$ be the smallest number with $\operatorname{ord}(w^n)$ finite. If $n = 1$, then the result follows from 3.2, and so we assume, for contrary, that $n \geq 2$. Since $S(+)$ is divisible, there are $v \in S$, $k \in \mathbb{N} \cup \{0\}$ and a polynomial $f(x) \in F(x) \cup \{0\}$ such that $w = 2v$ and $v = kw + wf(w)$. Hence $w^{n-1} = 2kw^{n-1} + 2w^{n-1}f(w)$. By our assumption, $2w^{n-1}f(w)$ is of finite order. If $k = 0$, then clearly $\operatorname{ord}(w^{n-1})$ is finite, and if $k \geq 1$, then $\operatorname{ord}(w^{n-1})$ is finite as well, by 2.2, the final contradiction. □

Proposition 4.3.

(i) *If $u \in S$ is such that $w = wu$, then $u = 1_S$.*

(ii) *$1_S \in S$ (i.e. S is unitary) if and only if $S^2 = S$. In this case there exists w^{-1} in S and $S^n = S^m$ for all $n, m \in \mathbb{N}$ (here $S^k = \langle\{a_1 \dots a_k \mid a_i \in S\}\rangle$ for $k \in \mathbb{N}$).*

Proof.

(i) Let $w = wu$. Since $S = \mathcal{D}(S)w$, for every $a \in S$ there is $\alpha_a \in \mathcal{D}(S)$ such that $a = \alpha_a w$. Hence $a = \alpha_a w = \alpha_a wu = au$ for every $a \in S$. Thus $u = 1_S$.

(ii) Let $S^2 = S$. Then $w \in S = S^2$ and there is a non-zero polynomial $f(x) \in F(x)$ such that $w = wf(w)$. By (i), $f(w) = 1_S$. Now, since $1_S \in S = S^2$, we have, similarly, that $1_S = wv$ for some $v \in S$. Hence $w^{-1} = v \in S$. The rest is obvious. □

Lemma 4.1. *Let $k \in \mathbb{N}$, $k \geq 2$ and $u \in S \cup \{0\}$ be such that $w = kw + u$. Then there exists $v \in S \cup \{0\}$ such that $a = 2a + va$ for every $a \in S$.*

Proof. Let $u = mw + wf(w)$, where $m \in \mathbb{N} \cup \{0\}$ and $f(x) \in F(x) \cup \{0\}$. If $f(x) = 0$, then $\operatorname{ord}(w)$ is finite, S is idempotent by 3.2 and we can put $v = 0$.

Hence assume that $f(x) \neq 0$. Put $n = m + k$ and $b = f(w) \in S$. We have $w = nw + wb$. Adding $(n-2)w$ to both sides of this equality, we get $(n-1)w = 2(n-1)w + wb$. Since w is a generator and S is additively divisible, we have $b = (n-1)v$ for some $v \in S$. For every $a \in S$ there is $\alpha_a \in \mathcal{D}(S)$ such that $a = (n-1)\alpha_a w$. Hence $a = \alpha_a(n-1)w = \alpha_a(2(n-1)w + (n-1)wv) = 2a + av$ for every $a \in S$. □

Theorem 4.1. *If $1_S \notin S$, then there exists $v \in S \cup \{0\}$ such that $\{a + va \mid a \in S\}$ is an ideal in S consisting of idempotent elements.*

Proof. Since S is divisible, there is $f \in F(x)$ such that $w = 2f(w)$. By 4.3(ii), we get that $f(x) = kx + g(x)$ for some $k \in \mathbb{N}$, $k \geq 2$ and $g \in F(x) \cup \{0\}$. Now, by 4.1, there is $v \in S \cup \{0\}$ such that $a = 2a + va$ for every $a \in S$. Finally, $a + va$ is idempotent for every $a \in S$ by 1. □

Surprisingly, the assumption of not having a unit allows to prove more in 4.1. Such a situation is not too common. To illustrate some other cases and techniques that support the Conjecture 1.1(A) see the Examples 2.

***Examples* 2.**

(i) Since S is additively divisible, there are polynomials $f_n(x) \in F(x)$, for $n \in \mathbb{N}$, such that $w = nf_n(w)$. If the degrees of the polynomials f_n are bounded by a common constant, we get that S is additively idempotent, by 3.1.

(ii) Let $n, m, k, l \in \mathbb{N}$ be such that $n^{l-1} \neq m^{k-1}$ and suppose that $w = nw^k$ and $w = mw^l$. Then S has a unit and is additively idempotent. Indeed, $nm^k w^{kl} = n(mw^l)^k = nw^k = w = mw^l = m(nw^k)^l = mn^l w^{kl}$. Since $nm^k \neq mn^l$, the element w^{kl} is of finite order and S is additively idempotent by 4.2.

(iii) Let $w = 2(w + w^2)$ and $w = 3(w + w^3)$. Then S is additively idempotent again. To show it, add first these two equalities to obtain $2w = 5w + 2w^2 + 3w^3$. Now, since $w^2 = 2w^2 + 2w^3$ we can substitute in $2w = 5w + (2w^2 + 2w^3) + w^3 = 5w + w^2 + w^3$. Hence $4w = 10w + (2w^2 + 2w^3)$ and by the same substitution we get $4w = 10w + w^2$. Finally, $8w = 20w + 2w^2 = 18w + (2w + 2w^2) = 19w$ and w is of finite order. Thus S is additively idempotent by 4.2.

5. Conclusion

Proof of 1.1. First, it is clear that (A) $\Longrightarrow$ (A1), (B) $\Longrightarrow$ (B1) and (A) $\Longrightarrow$ (B2). Furthermore, (C) $\Longleftrightarrow$ (C1) by [15: 5.1]. Now, assume that (A1) is true and let S be a finitely generated additively divisible semiring. By 3.2.4(ii), S/σ_S is additively uniquely divisible and, of course, this semiring inherits the property of being finitely generated. By (A1), the semiring S/σ_S is additively idempotent, and hence the semiring S is additively torsion by 3.2.4(i). Finally, S is additively idempotent by 3.1.1. We have shown that (A1) $\Longrightarrow$ (A) and consequently, (A) $\Longleftrightarrow$ (A1).

Next, let (B1) be true and let S be a finitely generated semiring containing a subsemiring $Q \cong \mathbb{Q}^+$. Put $P = S \cdot 1_Q$. Then P is an ideal of S, $1_Q = 1_P$, $Q \subseteq P$ and the map $s \mapsto s1_Q$ is a homomorphism of S onto P. Thus P is a finitely generated semiring and this is a contradiction with (B1). We have shown that (B1) $\Longrightarrow$ (B) and consequently, (B) $\Longleftrightarrow$ (B1).

The implication (B2) $\Longrightarrow$ (B1) is easy, since every semiring S with a unit element 1_S that contains a subsemiring $Q \cong \mathbb{Q}^+$ with $1_S = 1_{\mathbb{Q}^+}$ is additively divisible (for $a \in S$ and $m \in \mathbb{N}$ choose $b = (m1_S)^{-1}a \in S$ and get $a = mb$).

The implication (B) $\Longrightarrow$ (B2) follows immediately from 3.2.2.

We have shown that (B) $\Longrightarrow$ (B2) $\Longrightarrow$ (B1) $\Longleftrightarrow$ (B).

Finally, the implication (B2) $\Longrightarrow$ (C) follows from the fact that every parasemifield S is additively divisible, since the prime parasemifield of S containing 1_S is isomorphic either to $\mathbb{Q}^+$ or to the trivial semiring. □

Remark 2. Let us modify the assertion of 1.1 by omitting the statement (C1) and, for a fixed $n \in \mathbb{N}$, substituting "finitely generated" by "n-generated" in the statements of 1.1. Notice that in this case the proof of 1.1 works as well.

Remark 3. Note that using the Birkhoff's theorem we can consider an equivalent version of the conjecture (A):

(A') Every finitely generated subdirectly irreducible additively divisible semiring is additively idempotent.

Of course, it would be sufficient if such a semiring was finite. Unfortunately, this is not true. Take for instance the tropical semiring – the set of integers $\mathbb{Z}$ equipped with $a \oplus b = \min\{a, b\}$ as addition and $a \odot b = a + b$ as multiplication for $a, b \in \mathbb{Z}$ (this semiring is two-generated and has just two congruences). Nevertheless, it is an open question whether also one-generated subdirectly irreducible additively divisible semiring can be infinite.

Finally, Mal'cev [18] proved that every finitely generated commutative semigroup is residually finite (i.e. it is a subdirect product of finite semigroups). Notice, that also the additive part of a finitely generated free additively idempotent semiring is a residually finite semigroup. If this is true also for every finitely generated additively divisible semiring, we get a nice positive answer to the conjecture (A).

REFERENCES

[1] BASHIR, R. EL—HURT, J.—JANČAŘÍK, A.—KEPKA, T.: *Simple commutative semirings*, J. Algebra **236** (2001), 277–306.

[2] BENNINGFIELD, K.: *Cancellation and embedding theorems for compact uniquely divisible semigroups*, Semigroup Forum **58** (1999), 336–347.

[3] BROWN, D. R.—FRIEDBERG, M.: *Representation theorems for uniquely divisible semigroups*, Duke Math. J. **35** (1968), 341–352.

[4] BROWN, D. R.—FRIEDBERG, M.: *A survey of compact divisible commutative semigroups*, Semigroup Forum **1** (1970), 143–161.

[5] BROWN, D. R.—FRIEDBERG, M.: *Linear representations of certain compact semigroups*, Trans. Amer. Math. Soc. **160** (1971), 453–465.

[6] BROWN, D. R.—HILDEBRANT, J. A.: *Embedding compact t-semigroups into compact uniquely divisible semigroups*, Semigroup Forum **41** (1990), 61–82.

[7] BROWN, D. R.—LATORRE, J. G.: *A characterization of uniquely divisible commutative semigroups*, Pacific J. Math. **18** (1966), 57–60.

[8] BROWN, D. R.—STEPP, J. W.: *The structure semilattice of a compact UDC semigroup*, Semigroup Forum **31** (1985), 235–250.

[9] CLARK, W. E.—HOLLAND, W. C.—SZÉKELY, G. J.: *Decompositions in discrete semigroups*, Studia Sci. Math. Hungar. **34** (1998), 15–23.

[10] DEVUN, E. E.—GRAHAM, G.: *Semigroups with commuting threads*, Semigroup Forum **39** (1989), 203–213.

[11] FRIEDBERG, M.: *Homomorphisms of divisible semigroups*, Math. Z. **123** (1971), 215–218.

[12] GUBA, V. S.: *A finitely generated complete group*, Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986), 883–924 (Russian) [English translation: Math. USSR Izv. **29** (1987), 233–277].

[13] HILDEBRANT, J. A.: *On compact divisible abelian semigroups*, Proc. Amer. Math. Soc. **19** (1968), 405–410.

[14] JEŽEK, J.—KALA, V.—KEPKA, T.: *Finitely generated algebraic structures with various divisibility conditions*, Forum Math. **24** (2012), 379–397.

[15] KALA, V.—KEPKA, T.: *A note on finitely generated ideal-simple commutative semirings*, Comment. Math. Univ. Carolin. **49** (2008), 1–9.

[16] KALA, V.—KEPKA, T.—KORBELÁŘ, M.: *Notes on commutative parasemifields*, Comment. Math. Univ. Carolin. **50** (2009), 521–533.

[17] KARVELLAS, P. H.: *Additive divisibility in compact topological semirings*, Canad. J. Math. **26** (1974), 593–599.

[18] MAL'CEV, A. I.: *On homomorphisms into finite groups*, Ucheb. Zap. Ivanovsk. Gos. Ped. Inst. **18** (1958), 49–60 (Russian) [English translation: In: Twelve Papers in Algebra (L. J. Leifman, ed.), Amer. Math. Soc. Transl. Ser. 2 Vol. 119, Amer. Math. Soc., Providence, RI, 1983, pp 67–79].

[19] OLSHANSKII, A. YU.: *Geometry of Defining Relations in Groups*, Nauka, Moscow, 1989 (Russian) [English translation: Kluwer, Dordrecht, 1991].

[20] TAMURA, T.: *Minimal commutative divisible semigroups*, Bull. Amer. Math. Soc. **69** (1963), 713–716.

Received 30. 1. 2014
Accepted 19. 9. 2014

* *Department of Algebra*
Faculty of Mathematics and Physics
Charles University
Sokolovská 83
186 75 Prague 8
CZECH REPUBLIC
E-mail: Tomas.Kepka@mff.cuni.cz

** *Department of Mathematics and Statistics*
Faculty of Science
Masaryk University
Kotlářská 2
611 37 Brno
CZECH REPUBLIC
E-mail: miroslav.korbelar@gmail.com

Journal of Algebra and Its Applications
Vol. 16, No. 2 (2017) 1750038 (22 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0219498817500384

One-generated semirings and additive divisibility

Miroslav Korbelář*

Department of Mathematics and Statistics
Faculty of Science, Masaryk University
Kotlářská 2, 611 37 Brno, Czech Republic
**miroslav.korbelar@gmail.com*

Günter Landsmann

Research Institute for Symbolic Computation
Johannes Kepler University, Altenbergerstr. 69
A-4040 Linz, Austria
landsmann@risc.jku.at

Received 13 January 2016
Accepted 7 February 2016
Published 30 March 2016

Communicated by L. H. Rowen

We study the structure of one-generated semirings from the symbolical point of view and their connections to numerical semigroups. We prove that such a semiring is additively divisible if and only if it is additively idempotent. We also show that every at most countable commutative semigroup is contained in the additive part of some one-generated semiring.

Keywords: Commutative semiring; divisible semigroup; idempotent; numerical semigroup; embedding.

Mathematics Subject Classification 2010: 16Y60, 12Y05, 20M14

1. Introduction

Commutative semirings became widely used in different parts of pure and applied mathematics (for an extensive overview and introduction to the theory see [6, 7, 9]). An important milestone in the study of their basic properties was the classification of simple semirings [4] (for a more recent result in non-commutative semirings see [17]). This research further motivated a series of quite strong conjectures stated in [13] and claiming that every finitely generated additively divisible semiring (possibly with unit) is additively idempotent. With the additional assumption that the multiplicative part is a group, these conjectures have been confirmed for the at most two-generated case in [10, 12]. First steps toward the general cases have been

*Corresponding author.

made in [13]. Equivalent expressions of these problems in terms of free commutative semirings are as follows.

Conjecture 1.1. *Let $k \in \mathbb{N}$ and $\{f_{i,n} \,|\, n \in \mathbb{N} \,\&\, i = 1, \dots, k\} \subseteq \mathbb{N}[x_1, \dots, x_k]$ be a set of polynomials that have zero constant terms. The system of relations*

$$x_i \equiv n \cdot f_{i,n}(x_1, \dots, x_k) \quad \textit{where} \quad n \in \mathbb{N}, \quad i = 1, \dots, k$$

implies relations $x_i \equiv 2 \cdot x_i$ for all $i = 1, \dots, k$ by using only addition and multiplication in $\mathbb{N}[x_1, \dots, x_k]$.

Conjecture 1.2. *Let $k \in \mathbb{N}$ and $\{f_n \,|\, n \in \mathbb{N}\} \subseteq \mathbb{N}[x_1, \dots, x_k]$ be a set of polynomials. The system of relations*

$$1 \equiv n \cdot f_n(x_1, \dots, x_k) \quad \textit{where } n \in \mathbb{N}$$

implies relation $1 \equiv 2$ by using only addition and multiplication in $\mathbb{N}[x_1, \dots, x_k]$.

This formulation suggests to approach these problems from a computational point of view (for rewriting techniques in semirings see e.g. [1, 14]). In this paper we use some types of rewriting in the free semiring $\mathbb{N}[x]$ that will help us to understand better the structure of one-generated semirings in the context of numerical semigroups. We give affirmative answers for the one-generated case of both Conjectures 1.1 and 1.2. Surprisingly, in the cases where the generator is not invertible, the proof is easier, since the system of relations describing the additive divisibility is more restricted. In the second part of our paper we show that every at most countable commutative semigroup is contained in the additive part of some one-generated semiring.

We believe that our approach will be useful for further study (not only of semirings) and its detailed description may bring suggestions how to attack both of the conjectures for cases with more generators. Therefore we bring full proofs of all the auxiliary statements needed.

The main idea of proving the Conjectures 1 and 2 for the one-generated case is the following: To show idempotency of a semiring S it is enough to check that a generator $w \in S$ is torsion (Theorem 5.1). This is easy (Proposition 5.1), if there is some common bound of the degree for infinitely many polynomials $f_n \in \mathbb{N}[x]$ such that $1_S = n \cdot f_n(w)$. Fortunately, we can almost always reduce the degree of such polynomials using a particular rewriting algorithm (Lemma 4.4).

2. Preliminaries

Throughout this paper, a semiring S will be a non-empty set equipped with two commutative and associative binary operations, an addition and a multiplication, such that the multiplication distributes over the addition. Due to the more traditional notion of a semiring in computational mathematics, we will assume (in contrast to papers [4, 10, 11, 13]) that there is a multiplicatively neutral element in S (denoted as 1_S), unless we stress that this assumption is omitted.

We use the usual notation: $\mathbb{N}$ for the semiring of positive integers, $\mathbb{N}_0$ for the semiring of non-negative integers, $\mathbb{Z}$ for the ring of integers and $\mathbb{Q}$ for the ring of rational numbers.

For a set of variables X we denote $\mathbb{N}_0[X]$ the semiring of all polynomials with non-negative integer coefficients over the variables X. Further, we set $\mathbb{N}[X] := \mathbb{N}_0[X]\backslash\{0\}$ the subsemiring of $\mathbb{N}_0[X]$ consisting of all nonzero polynomials. The latter semiring $\mathbb{N}[X]$ is a free object with basis X in the category of all commutative semirings with units and with homomorphisms preserving these units. In this sense we say that a semiring S *is generated by a subset* $\{w_1, \dots, w_n\} \subseteq S$ iff $S = \{f(w_1, \dots, w_n) \mid f \in \mathbb{N}[x_1, \dots, x_n]\}$.

For a semiring $(S, +, \cdot)$ with additively neutral element 0 let $\langle D\rangle^+$ denote the submonoid of $(S, +)$ generated by the set $D \subseteq S$.

We will always consider the natural pre-order $\leq_S$ on the semiring S defined as

$$a \leq_S b \Leftrightarrow a = b \quad \text{or} \quad (\exists\, c \in S)\ a + c = b.$$

This pre-order is compatible with multiplication and addition and depends on the choice of the semiring (e.g. $2 \not\leq_{\mathbb{N}} 1$ in $(\mathbb{N}, +, \cdot)$ but $2 \leq_{\mathbb{Z}} 1$ in $(\mathbb{Z}, +, \cdot)$). The usual order in $\mathbb{Z}$ will be denoted as $\leq$.

The following notion establishes the connection between semirings and submonoids of $(\mathbb{N}_0, +)$.

Definition 2.1. Let S be a semiring. For $a \in S$ denote

$$\Pi_a(S) := \{k \in \mathbb{N}_0 \mid a^k \leq_S 1_S\}$$

the set of all powers of a that are contained in 1_S (with respect to S), and

$$\mathrm{Pol}_a := \{h \in \mathbb{N}[x] \mid h(a) = 1_S\}$$

the set of all polynomials expressing 1_S via the element $a \in S$. We will omit the reference to S in $\Pi_a(S)$ and write only Π_a if there is no confusion.

For $f = \sum_i a_i x^i \in \mathbb{N}_0[x]$ put $\pi(f) := \{k \in \mathbb{N}_0 \mid x^k \leq_{\mathbb{N}_0[x]} f\}$ the set of all powers of x that are contained in f. If $0 \neq f$ we denote $\mathrm{ldeg}(f) := \min(\pi(f))$ the least power of x appearing in f and $\mathrm{lc}(f) := a_{\deg(f)}$ the leading coefficient of f.

Proposition 2.1. *Let S be a semiring, $a \in S$. Then Π_a is a submonoid of $(\mathbb{N}_0, +)$.*

Proof. Clearly, $0 \in \Pi_a$. Let $k, \ell \in \Pi_a$. Then $1_S \geq_S a^k$ and $1_S \geq_S a^\ell$. Hence $1_S \geq_S a^k = 1_S \cdot a^k \geq_S a^\ell \cdot a^k = a^{k+\ell}$ and $k + \ell \in \Pi_a$. □

Proposition 2.2. *Let S be a semiring, $a \in S$. Let $g \in \mathrm{Pol}_a$ and $f_1, f_2 \in \mathbb{N}_0[x]$. Then*

(i) $1 \in \mathrm{Pol}_a$.
(ii) $f_1 + f_2 \in \mathrm{Pol}_a \Leftrightarrow f_1 g + f_2 \in \mathrm{Pol}_a$.
(iii) $1 + f_2 \in \mathrm{Pol}_a \Leftrightarrow 1 + f_1 + f_2 \in \mathrm{Pol}_a$, *if* $1 + f_1 \in \mathrm{Pol}_a$.

In particular, Pol_a *is a submonoid of* $(\mathbb{N}_0[x], \cdot)$ *and* $\bigcup_{f\in\mathrm{Pol}_a} \pi(f) \subseteq \Pi_a$.

Moreover, if S is generated by a then $\Pi_a = \bigcup_{f\in\mathrm{Pol}_a} \pi(f)$.

Proof. Conditions (i) and (ii) follow immediately from the definition. To show (iii), let $1 + f_1 \in \mathrm{Pol}_a$. By (ii), $1 + f_2 \in \mathrm{Pol}_a \Leftrightarrow 1 \cdot (1 + f_1) + f_2 \in \mathrm{Pol}_a$. The rest is easy. □

Remark 2.1. In the sequel we will need the following assertions that are either well known or are easy to verify.

(1) Every submonoid A of $(\mathbb{N}_0, +)$ is finitely generated and there is $n \in \mathbb{N}_0$ such that $d \cdot (n + \mathbb{N}_0) \subseteq A \subseteq d \cdot \mathbb{N}_0$, where $d = \gcd(A) \in \mathbb{N}_0$ (see e.g. [15]).

(2) In every idempotent semiring the natural pre-order is an order (see e.g. [8]).

(3) Let S be a semiring generated by $w \in S$ and $\gcd(\Pi_w(S)) = d > 0$. Then the relation $\equiv_{S,d}$ on $\mathbb{N}[x]$, defined as

$$f(x) \equiv_{S,d} g(x) \Leftrightarrow f(w^d) = g(w^d) \quad \text{for every } f, g \in \mathbb{N}[x]+$$

is a semiring congruence on $\mathbb{N}[x]$. For $\overline{S} := \mathbb{N}[x]_{/\equiv_{S,d}}$ and $\overline{w} := x_{/\equiv_{S,d}} \in \overline{S}$, the following conditions hold:

- $f(\overline{w}) = g(\overline{w}) \Leftrightarrow f(w^d) = g(w^d)$ for every $f, g \in \mathbb{N}[x]$,
- $\mathrm{Pol}_{\overline{w}}(\overline{S}) = \{h(x) \in \mathbb{N}[x] \mid h(x^d) \in \mathrm{Pol}_w(S)\}$,
- $\Pi_w(S) = d \cdot \Pi_{\overline{w}}(\overline{S})$,
- $\gcd(\Pi_{\overline{w}}(\overline{S})) = 1$.

(4) Let T be a semiring (not necessarily with unit) and let $w \in T$. Then the relation $\equiv$ on $\mathbb{N}[x]$, defined as

$$f(x) \equiv g(x) \Leftrightarrow wf(w) = wg(w) \quad \text{for every } f, g \in \mathbb{N}[x],$$

is a semiring congruence on $\mathbb{N}[x]$. The semiring $\tilde{T} := \mathbb{N}[x]_{/\equiv}$ has a unit and is generated by $\tilde{w} := x_{/\equiv} \in \tilde{T}$. For every $f, g \in \mathbb{N}[x]$, the following conditions hold:

$$f(\tilde{w}) = g(\tilde{w}) \Leftrightarrow wf(w) = wg(w).$$

(5) Let S be a semiring and $a = a + b$ for some $a, b \in S$. Then $a = a + nb$ for every $n \in \mathbb{N}$.

(6) Let S be a semiring generated by $w \in S$. Then:

- $1_S \in S + S \Leftrightarrow (\exists f \in \mathrm{Pol}_w)\ f(1) \geq 2$.
- w is invertible $\Leftrightarrow (\exists f \in \mathrm{Pol}_w)\ \mathrm{ldeg}(f) \geq 1$ (see [13]).

3. Numerical Semigroups and Rewriting in the Free Semiring $\mathbb{N}[x]$

In this section we introduce such types of rewriting, which help us later to derive the main theorems. As a consequence we naturally obtain an interesting interplay between submonoids of $(\mathbb{N}_0, +)$ and polynomials from $\mathbb{N}[x]$ in the sense of "generating polynomials" (see Remark 3.2).

Let us now state the main types of rewriting.

Definition 3.1. Let $r = \sum_{k \in \mathbb{N}_0} \lambda_k x^k, s = \sum_{k \in \mathbb{N}_0} \mu_k x^k \in \mathbb{N}[x]$ (with $\lambda_k, \mu_k \in \mathbb{N}_0$) and $r', r'', s', h, f, g \in \mathbb{N}[x]$ be polynomials and $d \in \mathbb{N}_0$ be a non-negative number. We define the following types of rewriting:

(Ia)

$$r \xrightarrow{d;h} r'$$

if $r' = \lambda_d x^d h + (r - \lambda_d x^d)$ and $r' \neq r$.

(Ib)

$$(r, s) \xrightarrow{d;h} (r', s')$$

if $r' = \lambda_d x^d h + (r - \lambda_d x^d)$, $s' = \mu_d x^d h + (s - \mu_d x^d)$ and $(r', s') \neq (r, s)$.

(II)

$$r \xrightarrow[(f,g)]{} r''$$

if

- $\mathrm{lc}(f) \mid \mathrm{lc}(r)$,
- $\deg(g) < \deg(f) \leq \deg(r)$,
- $r \geq_{\mathbb{N}[x]} \frac{\mathrm{lc}(r)}{\mathrm{lc}(f)} x^\delta f$,
- $r'' = (r - \frac{\mathrm{lc}(r)}{\mathrm{lc}(f)} x^\delta f) + \frac{\mathrm{lc}(r)}{\mathrm{lc}(f)} x^\delta g$,

where $\delta = \deg(r) - \deg(f) \in \mathbb{N}_0$.

Remark 3.1. Under the conditions of Definition 3.1, we always have $\deg(r'') < \deg(r)$ in (II). If $a \in S$ is such that $h(a) = 1_S$ then $r'(a) = r(a)$ in (Ia), and if $a \in S$ is such that $f(a) = g(a)$ then $r''(a) = r(a)$ in (II). This is important since the rewriting will be used mainly for polynomials from Pol_a.

The main purpose of type (II) is decreasing the degree of a rewritten polynomial. This is done in a similar way as in the Buchberger algorithm. In contrast to it, types (Ia) and (Ib) generally increase the degrees. They are motivated by a demand to add new monomials into the given polynomial (as in Proposition 3.3 and consequently in Lemma 4.2) and to "blow up" its coefficients (as in Theorem 3.1). Finally, the crucial application is a tandem of types (Ia) and (II) in Lemma 4.4.

Adding new monomials (and also their eliminating) illustrates Fig. 1 where polynomial h substitutes exponent b_0 appearing in $\pi(f)$ by a new set of exponents $b_0 + \{a_0, \ldots, a_n\}$ that becomes be part of $\pi(f')$. This happens since $\mathrm{ldeg}(h) \geq 1$. In the case when $\mathrm{ldeg}(h) = 0$, the exponent b_0 remains in $\pi(f')$.

To study the behavior of rewriting (Ia) and (Ib) we introduce the notion of derived sequences. A link between these sequences for a couple of polynomials and a single polynomial provides Proposition 3.1.

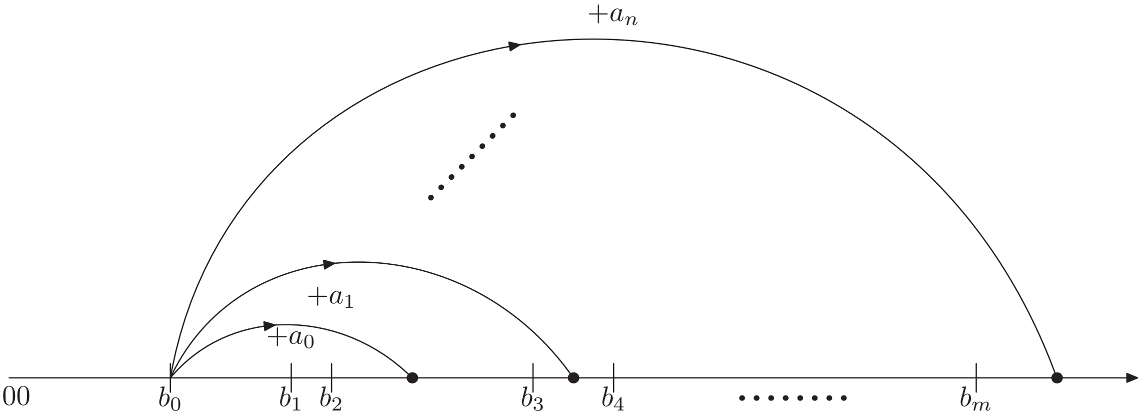


Fig. 1. Rewriting of type (Ia): $f \xrightarrow{b_0;h} f'$ where $\pi(f) = \{b_0, \dots, b_m\}$, $\pi(h) = \{a_0, \dots, a_n\}$ and $\text{ldeg}(h) \geq 1$.

Definition 3.2. Let $f, g, h \in \mathbb{N}[x]$ be polynomials and let $\deg(h) > 0$.

A sequence $\{(f_n, g_n, d_n) \,|\, n \in \mathbb{N}_0\} \subseteq \mathbb{N}[x] \times \mathbb{N}[x] \times \mathbb{N}_0$ defined recursively as

- $f_0 = f$, $g_0 = g$ and $d_0 = \min\{\text{ldeg}(f), \text{ldeg}(g)\}$,
- $(f_n, g_n) \xrightarrow{d_n;h} (f_{n+1}, g_{n+1})$ and $d_{n+1} = \min\{i \in \pi(f_{n+1}) \cup \pi(g_{n+1}) \,|\, i > d_n\}$ for $n \in \mathbb{N}_0$

will be called the *sequence derived from* (f, g) *by* h.

In the case when $f = g$ we (obviously) may use a shorter notation $\{(f_n, d_n) \,|\, n \in \mathbb{N}_0\} \subseteq \mathbb{N}[x] \times \mathbb{N}_0$ and call it the *sequence derived from* f *by* h.

Notice that since $\deg(h) > 0$ in Definition 3.2, both derived sequences are well defined.

Proposition 3.1. *Let* $r, s, h \in \mathbb{N}[x]$ *and* $\deg(h) > 0$. *Let* $\{(r_n, s_n, d_n) \,|\, n \in \mathbb{N}_0\}$ *be the sequence derived from* (r, s) *by* h. *Then* $\{(r_n + s_n, d_n) \,|\, n \in \mathbb{N}_0\}$ *is the sequence derived from* $r + s$ *by* h.

Moreover, the set $M = \{n \in \mathbb{N}_0 \,|\, r_n \neq r_{n+1}\}$ *is infinite. If* M *is listed as a strictly increasing sequence* $\{n_k\}_{k \in \mathbb{N}_0}$, *then* $\{(r_{n_k}, d_{n_k}) \,|\, k \in \mathbb{N}_0\}$ *is the sequence derived from* r *by* h.

Proof. Proof of the first claim goes easily by induction. The sequence $\{d_n\}_{n \in \mathbb{N}_0}$ is strictly increasing. Since $\deg(h) > 0$, we can, by construction of the derived sequence, immediately prove by induction that for every $n \in \mathbb{N}_0$ there are $i \in \pi(r_n)$ and $j \in \pi(s_n)$ such that $i, j \geq d_n$. This implies that the set $M = \{n \in \mathbb{N}_0 \,|\, r_{n+1} \neq r_n\}$ is infinite. Suppose now that we have a strictly increasing integer sequence $\{n_k\}_{k \in \mathbb{N}_0} \subseteq \mathbb{N}_0$ such that $M = \{n_k \,|\, k \in \mathbb{N}_0\}$.

By construction of the derived sequence, we clearly have that $r_{n_k} \xrightarrow{d_{n_k};h} r_{1+n_k} = r_{n_{k+1}}$ for every $k \in \mathbb{N}_0$.

To complete our proof we need to show that $d_{n_0} = \text{ldeg}(r_{n_0})$ and $d_{n_{k+1}} = \min\{i \in \pi(r_{n_{k+1}}) \,|\, i > d_{n_k}\}$ for every $k \in \mathbb{N}_0$. To do this at once, set $d_{-1} = -1$,

$n_{-1} = 0$ and $c_k = \min\{i \in \pi(r_{n_k}) \mid i > d_{n_{k-1}}\}$ for $k \in \mathbb{N}_0$. Then $c_0 = \operatorname{ldeg}(r_{n_0})$ and we are going to prove that $d_{n_k} = c_k$ for every $k \in \mathbb{N}_0$. If $n_k = 0$ for some $k \in \mathbb{N}_0$ we clearly have $k = 0$ and $d_{n_0} = d_0 = \operatorname{ldeg}(r_0) = \operatorname{ldeg}(r_{n_0})$, since $r_0 \neq r_1$ in this case. For the rest of the proof assume therefore for the given k, that $n_k > 0$.

Since $r_{n_k} \neq r_{1+n_k}$, we obtain that $d_{n_k} \in \pi(r_{n_k})$ and therefore $d_{n_k} \geq c_k$. From the monotonicity of the sequence $\{d_n\}_{n\in\mathbb{N}_0}$ there is $m \in \{n_{k-1}+1, n_{k-1}+2, \ldots, n_k\}$ such that $d_{m-1} < c_k \leq d_m$. Since $r_m = r_{n_k}$, we have $c_k \in \pi(r_{n_k}) = \pi(r_m)$ and therefore $c_k \geq d_m$ by the definition of d_m. Hence $d_m = c_k \in \pi(r_{n_k}) = \pi(r_m)$. This implies $r_m \neq r_{m+1}$ and hence we get $n_k = m$ by the choice of n_k. Thus $c_k = d_m = d_{n_k}$ and we are done. □

Now, let $h = \sum_{i=0}^{n} \lambda_i x^{a_i} \in \mathbb{N}[x]$ be a polynomial and $\lambda_0, \ldots, \lambda_n > 0$. It is useful to notice that the polynomials in the sequence derived from 1 by h imitate the way how the submonoid $\Pi = \langle\pi(h)\rangle^+$ of $(\mathbb{N}_0, +)$ is constructed from the generating set $\pi(h) = \{a_0, \ldots, a_n\}$. Indeed, every element of Π appears (at least once) in a node of the tree in Fig. 2. The edges of the tree labeled with "$+\,a_i$" represent adding the value a_i by moving down in the tree to one level lower.

The following lemma describes basic properties of the derived sequences. The proof is straightforward by an inductive argument.

Lemma 3.1. *Let $f, h \in \mathbb{N}[x], \Pi = \langle\pi(h)\rangle^+$ and $N = \deg(h) > 0$. Let $\{(f_n, d_n) \mid n \in \mathbb{N}_0\}$ be the sequence derived from f by h. Then for every $n \in \mathbb{N}_0$ we have*

(1) $d_n \in \pi(f_n)$,
(2) $\operatorname{ldeg}(f_n) = \begin{cases} \operatorname{ldeg}(f) & \text{if } \operatorname{ldeg}(h) = 0, \\ d_n & \text{if } \operatorname{ldeg}(h) \geq 1, \end{cases}$
(3) $\deg(f_{n+1}) = \max\{\deg(f), d_n + N\}$,
(4) $(\pi(f_n)\backslash\{d_n\}) \cup \{d_n + N\} \subseteq \pi(f_{n+1})$,
(5) $\{d_0, \ldots, d_n\} \subseteq \pi(f_n)$ *and* $f_n \leq_{\mathbb{N}[x]} f_{n+1}$, *if* $\operatorname{ldeg}(h) = 0$.

Proposition 3.2. *Let $f, h \in \mathbb{N}[x]$ and $\Pi = \langle\pi(h)\rangle^+$. Let $\{(f_n, d_n) \mid n \in \mathbb{N}_0\}$ be the sequence derived from f by h. Then*

$$\pi(f) + \Pi = \{d_n \mid n \in \mathbb{N}_0\}.$$

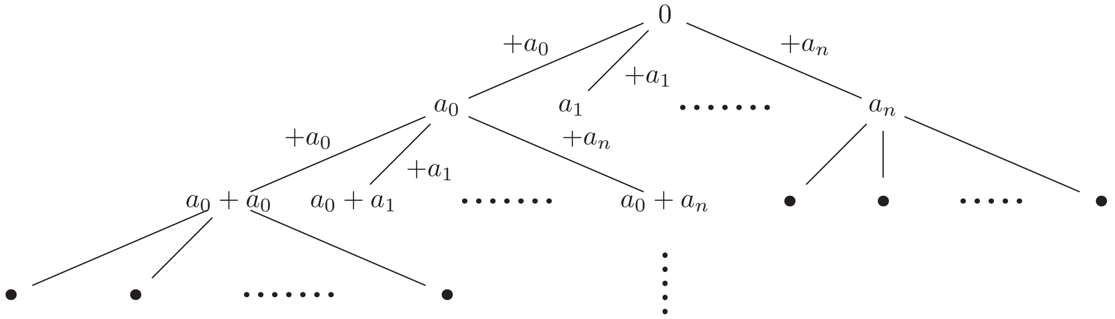


Fig. 2. The tree diagram of a monoid $(\langle a_0, \ldots, a_n\rangle^+, +)$.

Proof. First, observe that $\pi(f_m)\backslash\pi(f_n) \subseteq d_{n+1} + \mathbb{N}_0$ if $m > n$. This follows easily by induction using $A\backslash C \subseteq (A\backslash B) \cup (B\backslash C)$ for arbitrary sets A, B, C.

Now, we have $\Pi_1 := \{d_m \,|\, m \in \mathbb{N}_0\} \subseteq \bigcup_{n\in\mathbb{N}_0} \pi(f_n) \subseteq \Pi_2 := \pi(f) + \Pi$. To show that $\Pi_2 \subseteq \Pi_1$, assume the contrary. Let $a := \min(\Pi_2\backslash\Pi_1)$. Clearly, $a > 0$.

Since $a \in \Pi_2$, we have $a = b + k$, where either $b = 0$ and $0 \neq k \in \pi(f)$ or $b \in \Pi_2$ and $0 \neq k \in \pi(h)$. In the first case we have $a = k \in \pi(f) = \pi(f_0)$. In the second one we obtain $b \in \Pi_1$, since $b = a - k < a$, and therefore there is $m_0 \in \mathbb{N}_0$ such that $b = d_{m_0}$ and $a = b + k \in \pi(f_{m_0+1})$ by construction of f_{m_0+1}. Since $a \notin \Pi_1$, we get inductively, by Lemma 3.1(4), that $a \in \pi(f_m)$ for almost all $m \in \mathbb{N}_0$.

Now, there is $m_1 \in \mathbb{N}_0$ such that $d_{m_1} < a \leq d_{m_1+1}$. Since $a \notin \Pi_1$, we have $a \neq d_{m_1+1}$ and $a \notin \pi(f_{m_1})$, by the definition of d_{m_1+1}. Finally, we can choose $m_2 > m_1$ such that $a \in \pi(f_{m_2})\backslash\pi(f_{m_1})$. By our observation, we get $a \geq d_{m_1+1}$, a contradiction. □

In the case of numerical semigroups, polynomials in the derived sequence behave asymptotically quite simple properties — their monomials cover an interval within the semigroup and the appropriate coefficients increase above any limits (see Proposition 3.3 and Theorem 3.1). This observation is important for further applications in our paper — the main rewriting method for decreasing the degree of a polynomial (4.4) and dealing with the case of an invertible generator (Theorem 4.1).

Recall that a subsemigroup Π of the semigroup $(\mathbb{N}_0, +)$ is called *numerical* if $\mathbb{N}_0\backslash\Pi$ is a finite set (or equivalently, if $\gcd(\Pi) = 1$). Numerical semigroups appear in several branches of mathematics such as algebraic geometry or number theory. For more details see [3, 5, 15].

Proposition 3.3. *Let $f, h \in \mathbb{N}[x]$ be such that $\Pi = \langle\pi(h)\rangle^+$ is a numerical semigroup. Let $N = \deg(h)$ and let $\{(f_n, d_n) \,|\, n \in \mathbb{N}_0\}$ be the sequence derived from f by h.*

Then there is $n_0 \in \mathbb{N}$ such that for every $n \in \mathbb{N}_0, n \geq n_0$ we have

$$\pi(f_n) = \begin{cases} (\pi(f) + \Pi) \cap \{k \in \mathbb{N}_0 \,|\, k \leq \deg(f_n)\} & \textit{if } \operatorname{ldeg}(h) = 0, \\ d_n + \{0, 1, \ldots, N-1\} & \textit{if } \operatorname{ldeg}(h) \geq 1, \end{cases}$$

$\deg(f_n) = d_n + N - 1 = \deg(f_{n+1}) - 1$ *and* $d_n = d_{n-1} + 1$.

Proof. By Remark 2.1(1) there is $k_1 \in \mathbb{N}$ such that $k_1 + \mathbb{N}_0 \subseteq \pi(f) + \Pi$ and $\deg(f) \leq k_1$. By Proposition 3.2, there is $n_1 \in \mathbb{N}$ such that $d_{n_1} = k_1$ and $d_{n+1} = d_n + 1$ for every $n \geq n_1$.

First, we show by induction that for every $i \in \{0, \ldots, N-1\}$

$$d_{n_1} + \{i, N, N+1, \ldots, N+i-1\} \subseteq \pi(f_{i+n_1}).$$

For $i = 0$ this is obvious and for the induction step and $i + 1 < N$ it follows from Lemma 3.1(1) and Lemma 3.1(4) and the fact that $d_{k+n_1} = k + d_{n_1}$ for $k \in \mathbb{N}_0$. For $i = N - 1$ we therefore obtain $d_{N-1+n_1} + \{0, 1, \ldots, N-1\} \subseteq \pi(f_{N-1+n_1})$.

Now, set $n_0 = N - 1 + n_1$ and let $n \geq n_0$. Similarly as before we get

$$d_n + \{0, 1, \dots, N-1\} \subseteq \pi(f_n).$$

If $\operatorname{ldeg}(h) \geq 1$ we obtain $\pi(f_n) = d_n + \{0, 1, \dots, N-1\}$ by Lemma 3.1(1) and (2). In the remaining case, when $\operatorname{ldeg}(h) = 0$, we have $\{d_0, \dots, d_n\} \subseteq \pi(f_n)$, by Lemma 3.1(5). By Proposition 3.2, we further get $(\pi(f) + \Pi) \cap \{k \in \mathbb{N} \,|\, k \leq \deg(f_n)\} \subseteq \{d_i \,|\, i \in \mathbb{N}_0 \ \&\ d_i \leq \deg(f_n)\} \subseteq \{d_0, \dots, d_n\} \cup \{k \in \mathbb{N} \,|\, d_n \leq k \leq d_n + N - 1\} \subseteq \pi(f_n)$. The equality $\pi(f_n) = (\pi(f) + \Pi) \cap \{k \in \mathbb{N}_0 \,|\, k \leq \deg(f_n)\}$ now follows immediately. □

Definition 3.3. For $n \in \mathbb{N}_0$ put $\varepsilon_n := 1 + x + x^2 + \cdots + x^n \in \mathbb{N}[x]$.

Theorem 3.1. *Let $h \in \mathbb{N}[x]$ be such that $\Pi = \langle \pi(h) \rangle^+$ is a numerical semigroup, $N = \deg(h), \operatorname{ldeg}(h) \geq 1$ and $h(1) \geq 2$. Let $r, s \in \mathbb{N}[x]$ and $\{(r_n, s_n, d_n) \,|\, n \in \mathbb{N}_0\}$ be the sequence derived from (r, s) by h.*

Then for every $K > 0$ there is $n_K \in \mathbb{N}$ such that

$$r_n, s_n \geq_{\mathbb{N}[x]} K \cdot x^{d_n} \varepsilon_{N-1}$$

and

$$\pi(r_n) = \pi(s_n) = d_n + \{0, 1, \dots, N-1\}$$

for every $n \in \mathbb{N}, n \geq n_K$.

Proof. We prove our assertion for $K = 2^m$, $m \in \mathbb{N}_0$ by induction on m.

First, let $m = 0$. By Proposition 3.1, there is a sequence $\{p_k\}_{k \in \mathbb{N}_0} \subseteq \mathbb{N}_0$ such that the sequence $\{(r_{p_k}, d_{p_k}) \,|\, k \in \mathbb{N}_0\}$ is derived from r by h. By Proposition 3.3, there is k_0 such that $\pi(r_{p_k}) = d_{p_k} + \{0, 1, \dots, N-1\}$ and $d_{p_k} = d_{p_{k-1}} + 1$ for every $k \geq k_0$. Since the sequence $\{d_n\}_{n \in \mathbb{N}_0}$ is strictly increasing, we obtain that there is $n' \in \mathbb{N}$ such that $\pi(r_n) = d_n + \{0, 1, \dots, N-1\}$ for every $n \geq n'$. By a symmetric argument for s, we get that there is $n_1 \in \mathbb{N}$ such that $\pi(r_n) = \pi(s_n) = d_n + \{0, 1, \dots, N-1\}$ for every $n \geq n_1$.

Assume now that our assertion holds for $K = 2^m$. Since $h(1) \geq 2$, we get, by the first part, that there is $n_1' \in \mathbb{N}$ such that $\pi(r_n) = d_n + \{0, 1, \dots, N-1\}$ for every $n \geq n_1'$ and $r_{n_1'} = f + g$ for some $f, g \in \mathbb{N}[x]$. Clearly, the sequence $\{(r_{n_1'+k}, d_{n_1'+k}) \,|\, k \in \mathbb{N}_0\}$ is derived from $r_{n_1'}$ by h. By Proposition 3.1, there is a sequence $\{(f_k, g_k, e_k) \,|\, k \in \mathbb{N}_0\}$ derived from (f, g) by h such that $e_k = d_{n_1'+k}$ and $r_{n_1'+k} = f_k + g_k$ for every $k \in \mathbb{N}_0$. By our induction assumption there is $k_K \in \mathbb{N}$ such that $f_k, g_k \geq_{\mathbb{N}[x]} K \cdot x^{e_k} \varepsilon_{N-1}$ and $\pi(f_k) = \pi(g_k) = e_k + \{0, 1, \dots, N-1\}$ for every $k \in \mathbb{N}$, $k \geq k_K$. Hence for every $n \geq n_{2K}' := n_1' + k_K$ we get that $r_n = f_{n-n_1'} + g_{n-n_1'} \geq_{\mathbb{N}[x]} 2K \cdot x^{d_n} \varepsilon_{N-1}$ and $\pi(r_n) = d_n + \{0, 1, \dots, N-1\}$. By a symmetric argument we get the same property for the second polynomial s and our proof is done. □

Remark 3.2. Definitions 3.1 and 3.2 can be extended to polynomials from $\mathbb{R}_0^+[x]$. Let $f = \lambda_1 x^{a_1} + \cdots \lambda_n x^{a_n} \in \mathbb{R}_0^+[x]$ where $a_1, \dots, a_n \in \mathbb{N}$ and $\lambda_1, \dots, \lambda_n > 0$

and $\Pi = \langle a_1, \ldots, a_n \rangle^+$ be the submonoid of $(\mathbb{N}_0, +)$. Fixing the generating set $\{a_1, \ldots, a_n\}$, for $a \in \Pi$ let $\mathrm{Comb}_a = \{(k_1, \ldots, k_n) \in (\mathbb{N}_0)^n \mid a = \sum_{i=1}^n k_i a_i\}$ denote all the possible combinations of $\{a_1, \ldots, a_n\}$ expressing a and put

$$\Lambda_a = \sum_{(k_1,\ldots,k_n)\in\mathrm{Comb}_a} \lambda_1^{k_1} \cdots \lambda_n^{k_n}.$$

Now, let $\{(f_n, d_n) \mid n \in \mathbb{N}_0\}$ be the sequence derived from 1 by $1 + f$. One can show that within the power-series semiring $\mathbb{R}_0^+[[x]]$ we have

$$\lim_{n\to\infty} f_n = \sum_{a\in\Pi} \Lambda_a x^a.$$

Moreover, the sequence derived from 1 by f is of a similar form $\{(\tilde{f}_n, d_n) \mid n \in \mathbb{N}_0\}$ and the coefficient of the least monomial appearing in $\tilde{f}_n$ (i.e. of the monomial x^{d_n}) is equal to Λ_{d_n} for every $n \in \mathbb{N}_0$ and all elements of Π are listed in this way, i.e. $\Pi = \{d_n \mid n \in \mathbb{N}_0\}$, by Proposition 3.2.

4. Applications of Rewriting for One-Generated Semirings

Through this section, let S always be a semiring generated by $w \in S$, i.e. $S = \{f(w) \mid f \in \mathbb{N}[x]\}$. Our main aim here is to show that "most" of the elements of the form $(k \cdot 1_S)^{-1}$, where $k \in \mathbb{N}$, are contained in some "restricted area" (see Lemma 4.2).

We achieve this by decreasing the degree of the appropriate polynomial expressions of these elements. Since in semirings we cannot use subtraction, we "blow up" coefficients of the polynomial using rewriting of type (Ia) first and then we use rewriting of type (II) to decrease the degree (see Lemma 4.4).

For this purpose we need a key property of S, namely that $1_S \geq_S 2 \cdot 1_S$. This property can be easily derived when $\mathrm{ldeg}(f) = 0$ for every $f \in \mathrm{Pol}_w$ (i.e. w is *not* invertible, by Remark 2.1(6)), but in the opposite case, when there is an inverse to w, this property is not obvious at all. Therefore we have to guarantee it by Theorem 4.1, which provides even a much stronger information. Namely, it gives a full characterization of the case when the generator w of S is invertible and the canonical pre-order merges all elements.

First, in Lemma 4.1 we concentrate properties of Pol_w into a single polynomial.

Lemma 4.1. *Let $1_S \in S + S$. Then there is $g \in \mathrm{Pol}_w$ such that* $\gcd(\pi(g)) = \gcd(\Pi_w)$ *and $g(1) \geq 2$. Moreover*:

(1) *If there is $f_1 \in \mathrm{Pol}_w$ such that $\mathrm{ldeg}(f_1) \geq 1$, then g can be chosen with $\mathrm{ldeg}(g) \geq 1$.*
(2) *If there is $1 \neq f_2 \in \mathrm{Pol}_w$ such that $\mathrm{ldeg}(f_2) = 0$, then g can be chosen with $\mathrm{ldeg}(g) = 0$. If, in addition, $1_S \geq_S 2 \cdot 1_S$, then g can be chosen such that $\Pi_w = \langle \pi(g) \rangle^+$ and $g \geq_{\mathbb{N}[x]} 2$.*

Proof. By Remark 2.1(6), there is $f \in \mathrm{Pol}_w$ such that $f(1) \geq 2$. We can assume that f has at least one coefficient larger than 1, i.e. $f = 2x^k + r_0$ for some $k \in \mathbb{N}_0$ and $r_0 \in \mathbb{N}_0[x]$ (otherwise we take $f^2 \in \mathrm{Pol}_w$). Since Π_w is a semigroup, there are $a, b \in \Pi_w$ and $h_1, h_2 \in \mathrm{Pol}_w$ such that $d = a - b$, $h_1 \geq_{\mathbb{N}[x]} x^a$ and $h_2 \geq_{\mathbb{N}[x]} x^b$. Put $g_0 = x^k h_1 + x^k h_2 + r_0$. Clearly, $g_0(1) \geq 2$, $g_0 \geq_{\mathbb{N}[x]} x^k h_1 + x^k h_2 \geq_{\mathbb{N}[x]} x^{a+k} + x^{b+k}$ and $g_0 \in \mathrm{Pol}_w$, by Proposition 2.2. Since $a + k, b + k \in \pi(g_0)$ and $d = \gcd(\Pi_w) \leq \gcd(\pi(g_0)) \leq \gcd(a + k, b + k) = \gcd(a + k, (a + k) - (b + k)) \leq d$, we have $\gcd(\pi(g_0)) = d$.

(i) Now, let $f_1 \in \mathrm{Pol}_w$ and $\mathrm{ldeg}(f_1) \geq 1$. Put $g_1 = f_1 g_0$. Obviously, $g_1(1) \geq 2$, $\mathrm{ldeg}(g_1) \geq 1$ and $g_1 \in \mathrm{Pol}_w$, by Proposition 2.2. By construction of g_0, we have $a + n, b + n \in \pi(g_1)$ for some $n \in \mathbb{N}_0$. Since $g_1 \in \mathrm{Pol}_w$, we get $d = \gcd(\Pi_w) \leq \gcd(\pi(g_1)) \leq \gcd(a+n, b+n) = \gcd(a+n, (a+n)-(b+n)) \leq d$ similarly as before. Thus $\gcd(\pi(g_1)) = d$.

(ii) If $f_2 = 1 + s \in \mathrm{Pol}_w$ where $s \in \mathbb{N}[x]$ then, by Proposition 2.2, we have $g_2 = 1 \cdot g_0 + s \in \mathrm{Pol}_w$, $\gcd(\pi(g_2)) = d$, $\mathrm{ldeg}(g_2) = 0$ and $g_2(1) \geq 2$, again.

Assume now that $1_S \geq_S 2 \cdot 1_S$. By Remark 2.1(1), Π_w is generated by $a_1, \ldots, a_k \in \mathbb{N}_0$. Hence $1_S \geq_S w^{a_i}$ for every $i = 1, \ldots, k$. Since $1_S \geq_S 2 \cdot 1_S$, we have $1_S \geq_S n \cdot 1_S$ for every $n \in \mathbb{N}$. Thus $1_S \geq_S 2 \cdot 1_S + \sum_{i=1}^{k} 1_S \geq_S 2 \cdot 1_S + \sum_{i=1}^{k} w^{a_i}$ and there is $g_3 \in \mathrm{Pol}_w$ such that $\{a_1, \ldots, a_k\} \subseteq \pi(g_3)$, $g_3 \geq_{\mathbb{N}[x]} 2$ and $\Pi_w = \langle \pi(g_3) \rangle^+$.

□

The following lemma roughly says that if $1_S \geq_S 2 \cdot 1_S$, then Pol_w has "enough polynomials with large coefficients" (or that "every polynomial covered by Π_w can be covered by some polynomial from Pol_w").

Lemma 4.2. *Let* $\gcd(\Pi_w) = 1$ *and* $1_S \geq_S 2 \cdot 1_S$. *Then there is* $n_0 \in \mathbb{N}$ *such that for every* $r \in \mathbb{N}[x]$ *and* $n \in \mathbb{N}$ *with*

$$n \geq \max\{\deg(r), n_0\} \quad \textit{and} \quad \pi(r) \subseteq \Pi_w$$

there is $h \in \mathrm{Pol}_w$ *such that*

$$\deg(h) = n \quad \textit{and} \quad h \geq_{\mathbb{N}[x]} r + 1.$$

Proof. By Lemma 4.1(2), there is $s \in \mathbb{N}[x]$ such that $s \geq_{\mathbb{N}[x]} 2$, $s(w) = 1_S$ and $\Pi_w = \langle \pi(s) \rangle^+$. Let $\{(s_m, d_m) \mid m \in \mathbb{N}_0\}$ be the sequence derived from 1 by s. By Proposition 3.3 and Lemma 3.1(5), there is $n_1 \in \mathbb{N}$ such that for every $m \in \mathbb{N}$, $m \geq n_1$ is $s_m \in \mathrm{Pol}_w$, $\pi(s_m) = \Pi_w \cap \{0, 1, \ldots, \deg(s_m)\}$, $s_m \geq_{\mathbb{N}[x]} s_1 \geq_{\mathbb{N}[x]} 2$ and $\deg(s_{m+1}) = \deg(s_m) + 1$.

Put $n_0 = \deg(s_{n_1})$ and let $r \in \mathbb{N}[x]$ and $n \in \mathbb{N}$ be such that $n \geq \max\{\deg(r), n_0\}$ and $\pi(r) \subseteq \Pi_w$. Then there are $m \in \mathbb{N}$ and $t \in \mathbb{N}[x]$ such that $\deg(s_m) = n$ and $s_m = 2 + t$. Let K be the maximum of all coefficients of the polynomial $r + 1$. Since $\pi(r) \subseteq \Pi_w \cap \{0, 1, \ldots, \deg(s_m)\} = \pi(s_m)$, we have that $r + 1 \leq_{\mathbb{N}[x]} 1 + K(1 + t) \in \mathbb{N}[x]$. By Proposition 2.2(iii), $h = 1 + K(1 + t) \in \mathrm{Pol}_w$ is the desired polynomial.

□

In Lemma 4.3 we find a “universal” couple (f, g) for rewriting of the type (II).

Lemma 4.3. *Let* $\gcd(\Pi_w) = 1$. *Then there are* $f, g \in \mathbb{N}[x]$ *such that*

(1) $\deg(g) < \deg(f)$,
(2) $g(w) = f(w)$,
(3) $n + \pi(g), n + \pi(f) \subseteq \Pi_w$ *for every* $n \in \mathbb{N}_0$,
(4) $\mathrm{lc}(f) \mid \mathrm{lc}(h)$ *for every* $h \in \mathrm{Pol}_w$ *such that* $\deg(h) > 0$.

Proof. Since $\gcd(\Pi_w) = 1$, the set $\mathrm{Pol}_w^+ = \{h \in \mathrm{Pol}_w | \deg(h) > 0\}$ is non-empty. Let $d = \gcd\{\mathrm{lc}(h) \,|\, h \in \mathrm{Pol}_w^+\}$. Then there are $r_1, \dots, r_n \in \mathrm{Pol}_w^+$ and $s_1, \dots, s_m \in \mathrm{Pol}_w^+$ such that $d = d^+ - d^-$ where $d^+ = \sum_{i=1}^n \mathrm{lc}(r_i)$ and $d^- = \sum_{j=1}^m \mathrm{lc}(s_j)$. By Remark 2.1(1), there is $n_0 \in \mathbb{N}$ such that $n_0 + \mathbb{N}_0 \subseteq \Pi_w$. Hence we have $k_1, \dots, k_n \in n_0 + \mathbb{N}_0$ and $\ell_1, \dots, \ell_m \in n_0 + \mathbb{N}_0$ such that $\deg(x^{k_i} r_i) = \deg(x^{\ell_j} s_j)$ for all i and j.

Now, set $f_1 = \sum_{i=1}^n x^{k_i} r_i$, $g_1 = \sum_{i=1}^n x^{k_i}$, $f_2 = \sum_{j=1}^m x^{\ell_i} s_i$ and $g_2 = \sum_{j=1}^m x^{\ell_j}$. Then $\mathrm{lc}(f_1) = d^+$, $\mathrm{lc}(f_2) = d^-$ and $m := \deg(f_1) = \deg(f_2)$. Since $\deg(r_i) \geq 1$, $\deg(s_j) \geq 1$, $1_S = r_i(w)$ and $1_S = s_j(w)$ for all i and j, we have $\deg(f_p) > \deg(g_p)$ and $g_p(w) = f_p(w)$ for $p = 1, 2$. Further, $f_1 = d^+ x^m + h_1$ and $f_2 = d^- x^m + h_2$, for some $h_1, h_2 \in \mathbb{N}_0[x]$ such that $\deg(h_1) < m$, $\deg(h_2) < m$.

Finally, set $f = dx^m + g_2 + h_1$ and $g = g_1 + h_2$. Then

$$\begin{aligned} g(w) = g_1(w) + h_2(w) = f_1(w) + h_2(w) &= d^+ w^m + h_1(w) + h_2(w) \\ &= dw^m + (d^- w^n + h_2(w)) + h_1(w) \\ &= dw^m + f_2(w) + h_1(w) \\ &= dw^m + g_2(w) + h_1(w) = f(w). \end{aligned}$$

Obviously, (1), (2), (3) and (4) are true. □

Finally, Lemma 4.4 provides a method how the degree of a certain polynomial expression can be decreased. However, the coefficients in the resulting polynomial are increased on the other hand.

Lemma 4.4. *Let* $\gcd(\Pi_w) = 1$ *and* $1_S \geq_S 2 \cdot 1_S$.

Let $f, g \in \mathbb{N}[x]$ *be as in Lemma 4.3 and* n_0 *be as in Lemma 4.2. Set* $N = \max\{n_0, \deg(f)\} \in \mathbb{N}$. *Then for every* $r \in \mathbb{N}[x]$ *and* $k \in \mathbb{N}$ *fulfilling*

$$1_S = k \cdot r(w), \quad \gcd(k, \mathrm{lc}(f)) = 1, \quad r \geq_{\mathbb{N}[x]} 1 \quad \text{and} \quad \deg(r) > N$$

there are $h \in \mathrm{Pol}_w$ *and* $s, t \in \mathbb{N}[x]$ *such that*

$$r \xrightarrow{0;h} s \xrightarrow[(f,g)]{} t$$

and $\deg(r) = \deg(s) > \deg(t), t \geq_{\mathbb{N}[x]} 1, r(w) = s(w) = t(w)$.

Proof. Set $n_1 = \deg(f) \geq 1$ and $c = \mathrm{lc}(f)$. Let us now have $r \in \mathbb{N}[x]$ and $k \in \mathbb{N}$ such that $1_S = k \cdot r(w)$, $\gcd(k, c) = 1$, $r \geq_{\mathbb{N}[x]} 1$ and $\deg(r) > N$. Put $c' = \mathrm{lc}(r)$. By the choice of f, we have $c \mid kc'$. Thus $c' = cd$ for some $d \in \mathbb{N}$, since $\gcd(c, k) = 1$.

For $n = \deg(r)$ we have $n > N \geq n_1$ and therefore, by Lemma 4.3(3), $x^{n-n_1} f = c \cdot x^n + f_1$ for some $f_1 \in \mathbb{N}[x]$ such that $\deg(f_1) \leq n - 1$ and $\pi(f_1) \subseteq \Pi_w$. Since $n > N \geq n_0$, there is, by Lemma 4.2, $h \in \mathrm{Pol}_w$ such that $1 + d \cdot f_1 \leq_{\mathbb{N}[x]} h$ and $\deg(h) = n - 1$.

By the rewriting rule (Ia), there is $s \in \mathbb{N}[x]$ such that $r \xrightarrow{0;h} s$ and $\deg(s) = n$, $\mathrm{lc}(s) = c'$ and $s \geq_{\mathbb{N}[x]} h$. Hence $s \geq_{\mathbb{N}[x]} c'x^n$ and $s \geq_{\mathbb{N}[x]} h \geq_{\mathbb{N}[x]} d \cdot f_1 + 1$. Therefore we get $s \geq_{\mathbb{N}[x]} c'x^n + d \cdot f_1 + 1 = dx^{n-n_1} f + 1$. By the rewriting rule (II), there is $t \in \mathbb{N}[x]$ such that $s \xrightarrow[(f,g)]{} t \geq_{\mathbb{N}[x]} 1$, $\deg(t) < \deg(s) = \deg(r)$ and $t(w) = s(w) = r(w)$. □

Definition 4.1. We say that a semiring S *has a loop* if there are $a, b \in S$ such that $a = a + b$.

Theorem 4.1. *Let w be invertible in S. Then the following conditions are equivalent*:

(1) $a \geq_S b$ *for all* $a, b \in S$.
(2) $1_S \in S + S, \gcd(\Pi_w) = 1$ *and S has a loop.*

Proof. (1) ⇒ (2): Apply (1) on $a = 1_S$ and $b = 1_S + w$.

(ii) ⇒ (i): Let $a, b \in S$ and $f, g \in \mathbb{N}[x]$ be polynomials such that $a = f(w)$ and $b = g(w)$.

By Remark 2.1(2) and (6) and Lemma 4.1(1) there is $h \in \mathbb{N}[x]$ such that $\mathrm{ldeg}(h) \geq 1$, $\gcd(\pi(h)) = 1$, $h(1) \geq 2$ and $h(w) = 1_S$. Put $N = \deg(h)$.

Since S has a loop, there are $r, s \in \mathbb{N}[x]$ such that $r(w) = r(w) + s(w)$. Applying Theorem 3.1 on the couple (r, s), we get that there are $m \in \mathbb{N}$ and $\tilde{r}, \tilde{s} \in \mathbb{N}[x]$ such that $\tilde{s} \geq_{\mathbb{N}[x]} x^m \varepsilon_{N-1}$, $\pi(\tilde{r}) = \pi(\tilde{s}) = m + \{0, 1, \ldots, N-1\}$ and $\tilde{r}(w) = r(w)$, $\tilde{s}(w) = s(w)$. Hence, by Remark 2.1(5), we have $\tilde{r}(w) = \tilde{r}(w) + \ell \tilde{s}(w) \geq_S \ell \cdot w^m \varepsilon_{N-1}(w)$ for every $\ell \in \mathbb{N}$. Setting K as the maximum of all coefficients of the polynomial $\tilde{r}$ we have $K \cdot x^m \varepsilon_{N-1} \geq_{\mathbb{N}[x]} \tilde{r}$.

Further, applying Theorem 3.1 on the couple (f, g), there are $n \in \mathbb{N}$ and $\tilde{f}, \tilde{g} \in \mathbb{N}[x]$ such that $n \geq m$, $\tilde{f} \geq_{\mathbb{N}[x]} Kx^n \varepsilon_{N-1}$, $\pi(\tilde{f}) = \pi(\tilde{g}) = n + \{0, 1, \ldots, N-1\}$ and $\tilde{f}(w) = f(w) = a$, $\tilde{g}(w) = g(w) = b$. Setting L as the maximum of all coefficients of the polynomial $\tilde{g}$, we have $L \cdot x^n \varepsilon_{N-1} \geq_{\mathbb{N}[x]} \tilde{g}$.

Finally, we obtain

$$a = \tilde{f}(w) \geq_S K \cdot w^n \varepsilon_{N-1}(w) \geq_S w^{n-m} \tilde{r}(w) \geq_S L \cdot w^n \varepsilon_{N-1}(w) \geq_S \tilde{g}(w) = b$$

and we are done. □

In the context of the Theorem 4.1 let us note that the canonical pre-order can reach two extremes in semirings — either it merges everything (e.g. rings) or it is an order, in the so-called *dioids* [8] (e.g. idempotent semirings).

Corollary 4.1. *Let* $1_S \in S+S, \gcd(\Pi_w) = 1$ *and let* S *have a loop. Let* $k \in \mathbb{N}$. *If* $k \cdot 1_S$ *is invertible in* S, *then* $1_S \geq_S k \cdot 1_S$.

Proof. Let $k \cdot 1_S$ be invertible and $r \in \mathbb{N}[x]$ be such that $r(w) = (k \cdot 1_S)^{-1}$. Clearly, it is enough to show that $r(w) \geq_S 1_S$. If w is not invertible, then $\mathrm{ldeg}(r) = 0$, by Remark 2.1(6). Thus $r \geq_{\mathbb{N}[x]} 1$ and $r(w) \geq_S 1_S$. If w is invertible, then $r(w) \geq_S 1_S$, by Theorem 4.1. □

Theorem 4.2. *Let* $\gcd(\Pi_w) \in \{0,1\}$ *and let* S *have a loop. Then there are* $c \in \mathbb{N}$ *and* $N \in \mathbb{N}$ *such that*

$$(k \cdot 1_S)^{-1} \in \mathbb{N}_0 \cdot 1_S + \mathbb{N}_0 \cdot w + \cdots + \mathbb{N}_0 \cdot w^N$$

for every $k \in \mathbb{N}$, *with* $k \cdot 1_S$ *invertible and* $\gcd(k,c) = 1$.

Proof. Let $k \in \mathbb{N}$ and $a \in S$ be such that $1_S = (k \cdot 1_S) \cdot a = k \cdot a$.

First, assume that $1_S \notin S+S$. Then $\mathrm{Pol}_w \subseteq \{x^n \mid n \in \mathbb{N}_0\}$, by Remark 2.1(6). Thus we obviously have $k = 1$ and $(k \cdot 1_S)^{-1} = a = 1_S$. Hence we can set $c = 1$ and $N = 0$.

Now, if $\gcd(\Pi_w) = 0$ then $\mathrm{Pol}_w \subseteq \{\ell x^0 \mid \ell \in \mathbb{N}\}$. Therefore $(k \cdot 1_S)^{-1} = a \in \mathbb{N} \cdot 1_S$ and we can set $c = 1$ and $N = 0$ again.

Finally, suppose that $1_S \in S+S$ and $\gcd(\Pi_w) = 1$. Let N and f be as in Lemma 4.4. Set $c = \mathrm{lc}(f)$. Now, let $k \in \mathbb{N}$ be such that $\gcd(k,c) = 1$. By Corollary 4.1, we have $1_S \geq_S k \cdot 1_S$, i.e. $a = (k \cdot 1_S)^{-1} \geq_S 1_S$. Therefore there is $r \in \mathbb{N}[x]$ such that $a = r(w)$ and $r \geq_{\mathbb{N}[x]} 1$. Our assertion now follows immediately by using Lemma 4.4 repeatedly. □

5. One-Generated Divisible Semirings are Idempotent

In this section we finally confirm both Conjectures 1.1 and 1.2 for the case of one generator.

Let $(A,+)$ be a semigroup and $\emptyset \neq M \subseteq \mathbb{N}$ be a set. An element $a \in A$ is called *M-divisible* iff for every $n \in M$ there is $b \in A$ such that $a = \underbrace{b + \cdots + b}_{n\text{-times}}$.

A semiring $(S,+,\cdot)$ is called *additively divisible* iff every element of the additive semigroup $(S,+)$ is $\mathbb{N}$-divisible. A semiring $(S,+,\cdot)$ is called *additively idempotent* iff $a+a=a$ for every $a \in S$.

Proposition 5.1. *Let* $(A,+)$ *be a finitely generated commutative semigroup. Let* $M \subseteq \mathbb{N}$ *be an infinite set and* $\{v_m \in A \mid m \in M\}$ *be a subset of* A.

Then there are $\ell \in \mathbb{N}, m_1, \dots, m_\ell \in M$ and $c_1, \dots, c_\ell$, $d_1, \dots, d_\ell \in \mathbb{N}$ such that

$$\sum_{i=1}^{\ell} c_i m_i \cdot v_{m_i} = \sum_{i=1}^{\ell} d_i m_i \cdot v_{m_i} \quad \text{and} \quad \sum_{i=1}^{\ell} c_i \neq \sum_{i=1}^{\ell} d_i.$$

In particular, if $a \in A$ is M-divisible then a is torsion.

Proof. The first part of our assertion is enough to prove for finitely generated free commutative semigroups, i.e. for $A = \mathbb{N}_0^k \setminus \{\mathbf{0}\}$, $k \in \mathbb{N}$ and $\mathbf{0} = (0, \dots, 0) \in \mathbb{N}_0^k$.

Let W be the affine subspace of $\mathbb{Q}^k$ generated by the set $\{mv_m \mid m \in M\}$ and let $u \cdot v$ denote the standard scalar product of the vectors $u, v \in \mathbb{Q}^k$. We show that $\mathbf{0} \in W$. Assume the contrary. Then $W \neq \mathbb{Q}^k$ and there are $\mathbf{0} \neq u_0 \in \mathbb{Z}^k$ and $0 \neq d_0 \in \mathbb{Z}$ such that $u_0 \cdot w = d_0$ for every $w \in W$. Hence $u_0 \cdot (mv_m) = d_0$ and $m \mid d_0$ for every $m \in M$. Since M is infinite, we have $d_0 = 0$, a contradiction.

Now, since $\mathbf{0} \in W$, there are $\ell \in \mathbb{N}$, $m_1, \dots, m_\ell \in M$ and $e, c_1, \dots, c_\ell$, $d_1, \dots, d_\ell \in \mathbb{N}$ such that $\sum_{i=1}^{\ell} \frac{c_i - d_i}{e} \cdot m_i v_{m_i} = \mathbf{0}$ and $\sum_{i=1}^{\ell} \frac{c_i - d_i}{e} = 1$. Hence $\sum_{i=1}^{\ell} c_i m_i \cdot v_{m_i} = \sum_{i=1}^{\ell} d_i m_i \cdot v_{m_i}$ and $\sum_{i=1}^{\ell} c_i \neq \sum_{i=1}^{\ell} d_i$.

Finally, if $a \in A$ is M-divisible then for every $m \in M$ there is $u_m \in A$ such that $a = mu_m$. Hence, by our previous part, there are $\ell \in \mathbb{N}$, $m_1, \dots, m_\ell \in M$ and $c_1, \dots, c_\ell$, $d_1, \dots, d_\ell \in \mathbb{N}$ such that $c = \sum_{i=1}^{\ell} c_i \neq \sum_{i=1}^{\ell} d_i = d$ and $c \cdot a = \sum_{i=1}^{\ell} c_i a = \sum_{i=1}^{\ell} c_i m_i u_{m_i} = \sum_{i=1}^{\ell} d_i m_i u_{m_i} = \sum_{i=1}^{\ell} d_i a = d \cdot a$. Thus a is torsion. □

Theorem 5.1 ([13, 3.3]). *A finitely generated additively divisible semiring S is additively idempotent, provided that it is torsion.*

Theorem 5.2. *Every one-generated additively divisible semiring is additively idempotent. Moreover, if the generator is invertible then the semiring is finite.*

Proof. Let S be an additively divisible semiring generated by $w \in S$.

First, we show that S has a loop. The relation $\equiv$ on S, defined as $a \equiv b$ if and only if $a + z = b + z$ for some $z \in S$, is a semiring congruence of S and $\tilde{S} = S_{/\equiv}$ is again a finitely generated commutative semiring that is, moreover, additively cancellative. Hence the Grothendieck ring $G(S)$ of S, defined as the difference ring of $\tilde{S}$ (i.e. $G(S) = \tilde{S} - \tilde{S}$), is a finitely generated commutative ring and $\tilde{S}$ is a subsemiring of $G(S)$. Since $G(S)$ is additively divisible and finitely generated as well, it must be a trivial ring. Hence $1_S \equiv 1_S + 1_S$ and therefore there is $z \in S$ such that $1_S + z = 1_S + (1_S + z)$. Thus S has a loop.

Now, let us assume that $\gcd(\Pi_w) \in \{0, 1\}$ and let $c \in \mathbb{N}$ and $N \in \mathbb{N}$ be as in Theorem 4.2. Set $P = \{p \in \mathbb{P} \mid \gcd(p, c) = 1\}$ and let A be a subsemigroup of $(S, +)$ generated by $\{1_S, w, \dots, w^N\}$. By the divisibility of S and Theorem 4.2, for every $p \in P$ we have $(p \cdot 1_S)^{-1} \in A$, i.e. there is $a_p \in A$ such that $1_S = p \cdot a_p$. Hence 1_S is a P-divisible element of the finitely generated subsemigroup A. By Proposition 5.1, 1_S is torsion. Thus S is additively idempotent, by Theorem 5.1.

Consider now, in addition, for a while that w is invertible. By Remark 2.1(6) we have $\gcd(\Pi_w) > 0$, hence $\gcd(\Pi_w) = 1$. Since $1_S = 1_S + 1_S$, we get, by Theorem 4.1, that the natural pre-order $\leq_S$ is trivial. On the other hand $\leq_S$ has to be an order, by Remark 2.1(2). Thus S is a trivial semiring.

To complete our proof assume now that $\gcd(\Pi_w) = d > 0$. Let $\overline{S} = \mathbb{N}[x]_{/\equiv_{S,d}}$ and $\overline{w} = x_{/\equiv_{S,d}} \in \overline{S}$, where the relation $\equiv_{S,d}$ is defined in Remark 2.1(3). Then $\overline{S}$ is a semiring generated by $\overline{w}$ and $\gcd(\Pi_{\overline{w}}(\overline{S})) = 1$, by Remark 2.1(3). Since S is additively divisible, $\overline{S}$ is additively divisible as well. Thus, by the previous part of the proof, $1_{\overline{S}} = 1_{\overline{S}} + 1_{\overline{S}}$ (and $\overline{w} = 1_{\overline{S}}$ in case that w is invertible). Therefore $1_S = 1_S + 1_S$ (and $w^d = 1_S$ if w is invertible), by Remark 2.1(3), and S is additively idempotent (and finite if w is invertible), which concludes our proof. □

Corollary 5.1. *Let S be a semiring* (*not necessary with unit*) *and $w \in S$ be such that $S = \{f(w) \mid f \in x\mathbb{N}[x]\}$* (*i.e. S is generated by w in a more general sense*). *If S is additively divisible*, *then it is also additively idempotent.*

Proof. Follows immediately from Remark 2.1(4) and Theorem 5.2. □

6. Embedding of Semigroups into the Additive Part of Semirings

In this part we show that additive semigroups of finitely generated semirings are more colorful than those of rings, in the sense that every at most countable commutative semigroup is contained in the additive part of some finitely generated semiring (see Theorem 6.1 and Corollary 6.1). For this purpose we use a notion of strongly affine set, which preserves congruences of the additive part of a semiring (see Proposition 6.1).

Through this section let always $\{x_1, x_2, \ldots\}$ and $\{y_1, y_2, \ldots\}$ be mutually disjoint sets of pair-wise distinct variables. For $n \in \mathbb{N}$ put $F_n := \mathbb{N}_0[x_1, \ldots, x_n]$.

To simplify our notation, we set a few auxiliary notions.

Definition 6.1. Let $n \in \mathbb{N}$. For $\alpha = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ set $x^\alpha = x_1^{i_1} \ldots x_n^{i_n}$ and $|\alpha| = \sum_{k=1}^n i_k$. For $f \in F_n$ set

$$D_x(f) = \max\{|\alpha| | \alpha \in \mathbb{N}_0^n \,\&\, x^\alpha \leq_{F_n} f\}$$

the (*upper*) *graded degree of* f and

$$d_x(f) = \min\{|\alpha| | \alpha \in \mathbb{N}_0^n \,\&\, x^\alpha \leq_{F_n} f\}$$

the *lower graded degree of* f, if $f \neq 0$, otherwise put $D_x(f) = -\infty$ and $d_x(f) = \infty$.

A set $\emptyset \neq U \subseteq F_n$ will be called *strongly affine* $\Leftrightarrow$ for every $m \in \mathbb{N}$ and $f_1, \ldots, f_m \in U$ is every polynomial $\Phi \in F_n[y_1, \ldots, y_m]$, such that $\Phi(f_1, \ldots, f_m) \in \langle U \rangle^+$, of the form $\Phi(y_1, \ldots, y_m) = g + \sum_{i=1}^m k_i y_i$ for some $k_1, \ldots, k_m \in \mathbb{N}_0$ and $g \in \langle U \rangle^+$ (i.e. $\Phi \in \langle U \cup \{y_1, \ldots, y_n\} \rangle^+$).

Remark 6.1. It is easy to check that the following are equivalent for $\emptyset \neq U \subseteq F_n$, $n \in \mathbb{N}$:

(1) For every $m \in \mathbb{N}$, all *pair-wise distinct* $f_1, \dots, f_m \in U$ and every polynomial $\Phi \in F_n[y_1, \dots, y_m]$ such that $\Phi(f_1, \dots, f_m) \in \langle U \rangle^+$ is $\Phi \in \langle U \cup \{y_1, \dots, y_n\} \rangle^+$.
(2) U is strongly affine.
(3) $\langle U \rangle^+ \backslash \{0\}$ is strongly affine.

A strongly affine set allows to find an embedding of the additive semigroups.

Proposition 6.1. *Let $n \in \mathbb{N}, U \subseteq \mathbb{N}[x_1, \dots, x_n]$ be a strongly affine set and $G = \langle U \rangle^+ \backslash \{0\}$.*

Then $\overline{\rho} \cap (G \times G) = \rho$ for every semigroup congruence ρ of G, where $\overline{\rho}$ is the semiring congruence of $\mathbb{N}[x_1, \dots, x_n]$ generated by ρ.

In particular, $(G/_\rho, +)$ is a subsemigroup of $(\mathbb{N}[x_1, \dots, x_n]/_{\overline{\rho}}, +)$.

Proof. First, by Remark 6.1, G is also strongly affine.

Let ρ be a semigroup congruence of G. Clearly, $\overline{\rho} \cap (G \times G) \supseteq \rho$. To show the opposite inclusion we only need to prove the implication

$$(g, h \in G \,\&\, (g, h) \in \overline{\rho}) \Rightarrow (g, h) \in \rho$$

for the couples (g, h) of the form $g = \Phi(f_1, \dots, f_m)$ and $h = \Phi(\tilde{f}_1, \dots, \tilde{f}_m)$, where $m \in \mathbb{N}$, $\Phi \in F_n[y_1, \dots, y_m]$ and $(f_i, \tilde{f}_i) \in \rho$ for every $i = 1, \dots, m$.

Having now such a couple, we get, by assumption, that $\Phi = g_0 + \sum_{i=1}^m k_i y_i$ for some $k_i \in \mathbb{N}_0$ and $g_0 \in G$. Hence $g = g_0 + \sum_{i=1}^m k_i f_i$, $h = g_0 + \sum_{i=1}^m k_i \tilde{f}_i$ and $(g, h) \in \rho$, since ρ is a semigroup congruence on G. □

Proposition 6.2. *Let $n \in \mathbb{N}$.*

(1) *Let $\emptyset \neq V \subseteq U \subseteq F_n$. If U is strongly affine, then V is strongly affine and $0 \notin V$.*
(2) *The set $\{f\}$ is strongly affine for every $0 \neq f \in F_n$.*
(3) *The set $\{x_1, \dots, x_n\}$ is strongly affine.*

Proof. Follows easily using Remark 6.1. □

Lemma 6.1. *Let $n, k_0 \in \mathbb{N}_0$,*

$$A = \{f \in F_n \mid D_x(f) \leq k_0\}$$

and

$$B = \{x_1^{3^k} \in F_n \mid k_0 + 1 \leq k \in \mathbb{N}_0\}.$$

Set $H = \langle A \cup B \rangle^+$.

If $f \in H \backslash \bigcup_{j \in \mathbb{N}_0} \mathbb{N} x_1^j$, $0 \neq \alpha \in \mathbb{N}_0^n$ and there is $h \in H$ such that $x^\alpha f \leq_{F_n} h$ then $x^\alpha f \in A$.

Proof. Assume, for contrary that $D_x(x^\alpha f) > k_0$ for some $f \in H \setminus \bigcup_{j\in\mathbb{N}_0} \mathbb{N}x_1^j$ and $0 \neq \alpha \in \mathbb{N}_0^n$. Then, since $x^\alpha f + g \in H$ for some $g \in F_n$, there is $m \in \mathbb{N}$ such that $\alpha = (m, 0, \dots, 0) \in \mathbb{N}_0^n$ and f contains a monomial x_1^i, for some $i \in \mathbb{N}_0$, such that $m + i = 3^k$ where $k_0 + 1 \leq k \in \mathbb{N}$. By the definition of H, we either have $i \leq k_0$ or $i = 3^p$ for some $k_0 + 1 \leq p \in \mathbb{N}$. In the first case we get $i \leq k_0 < 3^{k_0} \leq 3^{k-1}$ and in the second case we get $3^p = i = 3^k - m < 3^k$ and $p < k$. Thus, we always have $i \leq 3^{k-1}$ and therefore $m = 3^k - i \geq 3^k - 3^{k-1} > 3^{k-1} \geq 3^{k_0} > k_0$. Hence $d_x(x^\alpha f) = d_x(x^\alpha) + d_x(f) \geq d_x(x^\alpha) = m > k_0$. It follows that $x^\alpha f \in \langle B\rangle^+$. By the definition of B and by the choice of f, f must now contain at least one another monomial x_1^j, with $i \neq j \in \mathbb{N}_0$. Since $x^\alpha f \in \langle B\rangle^+$, we get that $m + j = 3^\ell$ for some $k_0 + 1 \leq \ell \in \mathbb{N}$. Consequently, as before, $j \leq 3^{\ell-1}$.

Finally, we may assume, without loss of generality, that $i < j$. Then $k \leq \ell - 1$ and $3^{\ell-1} \geq j - i = 3^\ell - 3^k \geq 3^\ell - 3^{\ell-1} > 3^{\ell-1}$, a contradiction. □

The following assertion provides a sufficient condition when a strongly affine set with restricted graded degree can be extended to an infinite strongly affine set.

Proposition 6.3. *Let $n \in \mathbb{N}$ and $K \subseteq F_n$ be such that*

(1) $k_0 = \sup\{D_x(f) \mid f \in K\} < \infty$,
(2) *K is strongly affine*,
(3) $K \cap (\bigcup_{j\in\mathbb{N}_0} \mathbb{N}x_1^j) = \emptyset$.

Set $M = \{x_1^{3^{k_0+1}} + x_1^{3^k} \in F_n \mid k_0 + 1 < k \in \mathbb{N}\}$. Then $K \cup M$ is strongly affine.

Moreover, if K is a basis of the free commutative semigroup $\langle K\rangle^+ \setminus \{0\}$, then $K \cup M$ is a basis of the free commutative semigroup $\langle K \cup M\rangle^+ \setminus \{0\}$.

Proof. We divide the proof into four steps. Set $G = \langle K \cup M\rangle^+ \setminus \{0\}$. For $0 \leq m_0 \leq m \in \mathbb{N}$ let there be $f_1, \dots, f_{m_0} \in K$, $f_{m_0+1}, \dots, f_m \in M$ and $\Phi \in F_n[y_1, \dots, y_m]$ such that $\Phi(f_1, \dots, f_m) \in G$.

(1) Assume first, for contrary, that there is $i \in \{m_0 + 1, \dots, m\}$ such that the polynomial Φ (considered as an element of the semiring $R[y_i]$, where $R = F_n[y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_m]$) is either of degree higher than 1 in y_i or that the coefficient from R at y_i is different from a non-negative integer.

Then $x^\alpha f_i \leq_{F_n} \Phi(f_1, \dots, f_m) \in G$ for some $0 \neq \alpha \in \mathbb{N}_0^n$. By Lemma 6.1, we have $D_x(f_i) \leq D_x(x^\alpha) + D_x(f_i) = D_x(x^\alpha f_i) \leq k_0$, contradicting $f_i \in M$.

(2) Now, by part (1), there are polynomials $g \in F_n$, $\Psi_1 \in F_n[y_1, \dots, y_{m_0}]$ and $\Psi_2 \in \langle y_{m_0+1}, \dots, y_m\rangle^+$ such that Ψ_1 has a zero constant term and $\Phi(y_1, \dots, y_m) = \Psi_1(y_1, \dots, y_{m_0}) + \Psi_2(y_{m_0+1}, \dots, y_m) + g$.

Assuming further, for contrary, that $D_x(\Psi_1(f_1, \dots, f_{m_0})) > k_0$, there are $0 \neq \beta \in \mathbb{N}_0^n$ and $j \in \{1, \dots, m_0\}$ such that $x^\beta f_j \leq_{F_n} \Psi_1(f_1, \dots, f_{m_0}) \leq_{F_n} \Phi(f_1, \dots, f_m) \in G$ and $D_x(x^\beta f_j) > k_0$. By Lemma 6.1, we get again $D_x(x^\beta f_j) \leq k_0$, a contradiction.

Hence $D_x(\Psi_1(f_1,\dots,f_{m_0})) \le k_0$.

(3) Obviously, there are $g_1, g_2 \in F_n$ such that $g = g_1 + g_2$, $D_x(g_1) \le k_0$ and $d_x(g_2) > k_0$. Set $\Phi_1(y_1,\dots,y_{m_0}) = \Psi_1(y_1,\dots,y_{m_0}) + g_1$ and $\Phi_2(y_{m_0+1},\dots,y_m) = \Psi_2(y_{m_0+1},\dots,y_m) + g_2$. By (2) we have $D_x(\Phi_1(f_1,\dots,f_{m_0})) \le k_0$ and further is $d_x(\Phi_2(f_{m_0+1},\dots,f_m)) > k_0$. Hence we get that $\Phi_1(f_1,\dots,f_{m_0}) \in \langle K\rangle^+$ and $\Phi_2(f_{m_0+1},\dots,f_m) \in \langle M\rangle^+$.

Now, the set K is strongly affine and therefore $\Phi_1 \in \langle K \cup \{y_1,\dots,y_{m_0}\}\rangle^+$.

(4) Finally, assume that $g_2 \neq 0$. Both $\Phi_2(f_{m_0+1},\dots,f_m)$ and $\Psi_2(f_{m_0+1},\dots,f_m)$ belong to $\langle M\rangle^+ \subseteq F_n$. Hence there are $k \in \mathbb{N}$, $\ell_1,\dots,\ell_k \in \mathbb{Z}$ and pair-wise different $e_1,\dots,e_k \in M$ such that $g_2 = \Phi_2(f_{m_0+1},\dots,f_m) - \Psi_2(f_{m_0+1},\dots,f_m) = \sum_{p=1}^{k} \ell_p e_p \in \mathbb{Z}[x_1,\dots,x_n]$. But $g_2 \in F_n = \mathbb{N}[x_1,\dots,x_n]$ and $D_x(e_p) \neq D_x(e_q)$ for all $p \neq q$. Therefore $\ell_p \ge 0$ for all $p = 1,\dots,k$ and $g_2 \in \langle M\rangle^+$.

We conclude with $\Phi(y_1,\dots,y_m) = \Phi_1(y_1,\dots,y_{m_0}) + \Phi_2(y_{m_0+1},\dots,y_m) \in \langle K \cup M \cup \{y_1,\dots,y_m\}\rangle^+$.

The rest is easy. □

Finally, we show that not only every countable semigroup A can be embedded into the additive part of some finitely generated semiring S, but also that it can be done in a way that a given element of A may be mapped almost arbitrarily to S (resp. that A may contain almost all generators of S).

Theorem 6.1. *Let $(A,+)$ be an at most countable commutative semigroup, $n \in \mathbb{N}, a_1,\dots,a_n \in A$ and $f \in \mathbb{N}[x_1,\dots,x_n]$.*

If either $n \ge 2$ or f contains at least two different monomials, then there is a commutative semiring S generated by a set $\{w_1,\dots,w_n\} \subseteq S$ such that $(A,+)$ is a subsemigroup of $(S,+)$ and $f(w_1,\dots,w_n) = a_1$.

Moreover, if $n \ge 2$ and $f = x_1$ then S can be chosen such that $w_i = a_i$ for every $i = 1,\dots,n-1$.

Proof. First observe, that having an infinite strongly affine set $L = \{f_1, f_2, \dots\} \subseteq \mathbb{N}_0[x_1,\dots,x_n]$, such that L is a basis of the free commutative semigroup $G = \langle L\rangle^+ \setminus \{0\}$, there is an epimorphism $\varphi : (G,+) \to (A,+)$ such that $\varphi(f_i) = a_i$ for every $i \in \{1,\dots,n\}$. Set $\rho = \ker\varphi$ and let $\overline{\rho}$ be the semiring congruence of $\mathbb{N}[x_1,\dots,x_n]$ generated by ρ. Then, by Theorem 6.1, there is an embedding $\nu : (A,+) \cong (G_{/\rho},+) \hookrightarrow (\mathbb{N}[x_1,\dots,x_n]_{/\overline{\rho}},+)$ such that $\nu(a_i) = f_i/_{\overline{\rho}} = f_i(x_1/_{\overline{\rho}},\dots,x_n/_{\overline{\rho}})$ for every $i = 1,\dots,n$.

Now it remains to find a suitable set L. Put $k_0 = D_x(f)$.

For $n = 1$ and f that contains at least two different monomials set $L = \{f\} \cup \{x_1^{3^{k_0+1}} + x_1^{3^k} \mid k_0 + 1 < k \in \mathbb{N}\}$.

If $n \ge 2$ and $f \neq x_1$ then $f \notin \bigcup_{j\in\mathbb{N}_0} \mathbb{N}x_{i_0}^j$ for some $i_0 \in \{1,\dots,n\}$. In this case we set $L = \{f\} \cup \{x_{i_0}^{3^{k_0+1}} + x_{i_0}^{3^k} \mid k_0 + 1 < k \in \mathbb{N}\}$.

Finally, for $n \ge 2$ and $f = x_1$ we set $L = \{x_1,\dots,x_{n-1}\} \cup \{x_n^{3^{k_0+1}} + x_n^{3^k} \mid k_0 + 1 < k \in \mathbb{N}\}$.

Now, by Propositions 6.2 and 6.3, L is strongly affine and our proof is done. □

Let us still point out the following important fact.

Corollary 6.1. *Every at most countable commutative semigroup is contained in the additive part of some one-generated semiring.*

In view of Corollary 6.1, we may ask whether there is a single common one-generated semiring containing all such semigroups. This question is equivalent to an existence of a countable commutative semigroup that contains every at most countable commutative semigroup. Considering the case of groups only, there is such a group, namely the sum of countably many copies of the divisible group $\mathbb{Q} \oplus (\mathbb{Q}/\mathbb{Z})$, but in the case of semigroups a positive answer seems to be unlikely. Note that, according to [16], it is possible to reduce this problem to the case of divisible semigroups.

In the context of the Conjecture 1.1 it is now clear that in a semiring S generated by $\{w_1, \dots, w_k\} \subseteq S$ a system of equations

$$a = n \cdot f_n(w_1, \dots, w_k), n \in \mathbb{N}$$

where $a \in S$ and $\{f_n \in \mathbb{N}[x_1, \dots, x_k] \mid n \in \mathbb{N}\}$ is generally not enough to provide idempotency of a general element $a \in S$, even in the case when this element is torsion (simply choose the Prüfer group $A = \mathbb{Z}_{p^\infty}$ and use Theorem 6.1). This is a substantial difference to the case of finitely generated commutative rings where there are no additively divisible elements except zero.

7. Further Questions

In this paper we have shown that a list of relations $1 \equiv nf_n(x)$ where $f_n(x) \in \mathbb{N}[x]$, $n \in \mathbb{N}$ implies $1 \equiv 2$ in $\mathbb{N}[x]$. Although we have used a computational approach, our result is not purely algorithmic. Therefore the following questions are of interest.

Question 7.1. Let $\emptyset \neq M \subseteq \mathbb{N}[x]$ be a set and let $\equiv$ be a semiring congruence of $\mathbb{N}[x]$ generated by the set $\{1\} \times M$. Is there some rewriting system that decides whether $f(x) \equiv 1$ for given $f(x) \in \mathbb{N}[x]$?

Question 7.2. Having (a free commutative semiring) $F = \mathbb{N}[x_1, \dots, x_n]$ and a congruence $\equiv$ on F generated by a subset of $F \times F$, is there a rewriting system that decides whether $f \equiv g$ for given polynomials $f, g \in F$?

In the context of Question 7.1, let us still provide description of the semiring-congruence class that contains the unit.

Proposition 7.1. *The following conditions are equivalent for* $\emptyset \neq M \subseteq F = \mathbb{N}_0[x_1, \dots, x_k]$:

(1) $M = \{f \in F \mid f \equiv 1\}$ *where* $\equiv$ *is a semiring congruence on* F *generated by the set* $\{1\} \times M$.

(2) $1 \in M$ *and* $(\forall\, f_1, f_2 \in F)(\forall\, g \in M)\ f_1 + f_2 \in M \iff f_1 g + f_2 \in M$.

Proof. The implication (1)⇒(2) is easy. For the opposite direction we clearly have $M \subseteq \{f \in F \mid f \equiv 1\} =: \widetilde{M}$. We show inductively that $a \in \widetilde{M}$ belongs to M based on the number of couples from $\{1\} \times M$ that we need to connect a and 1 within the congruence $\equiv$. Let $b \in M$ be connected with a by $(1, g) \in \{1\} \times M$. Then there are $f_1, f_2 \in F$ such that either $a = f_1 + f_2$ and $b = f_1 g + f_2$ or that $a = f_1 g + f_2$ and $b = f_1 + f_2$. In both cases $a \in M$ and we are done. □

Based on the computational approach, it seems that the following generalization of Conjecture 1.1 might be true.

Conjecture 7.1. *Let S be a finitely generated commutative semiring and M be a finitely generated S-semimodule. If the semigroup M is divisible, then M is idempotent.*

This conjecture is also a natural generalization of the following fact: *Every finitely generated commutative semigroup (i.e. a finitely generated $\mathbb{N}$-semimodule) that is divisible, is also idempotent.* For the proof see e.g. [2].

Remark 7.1. Note that, according to Theorem 5.2, the Conjecture 7.1 holds when both S and M are one-generated. Indeed, let $m \in M$ be a generator of the S-semimodule M. We can assume without loss of generality that M is unitary as an S-semimodule (otherwise we add a unit to S freely). For $a, b \in S$ set $a \equiv b$ if and only if $am = bm$. Clearly, $\equiv$ is a congruence of the semiring S and $S_{/\equiv}$ is additively divisible, since M is so. By Theorem 5.2, $S_{/\equiv}$ is additively idempotent. Hence $m = 1_S m = 2 \cdot 1_S m = 2m$ and the semigroup M is idempotent as well.

Acknowledgments

The first author was supported by the Czech Science Foundation (GAČR) by Grant GP13-29835P. The second author was partially supported by the Austrian Science Fund (FWF): W1214-N15, Project DK11.

The authors also would like to thank Ondřej Klíma (Department of Mathematics and Statistics, Masaryk University in Brno) for his valuable suggestions and comments.

References

[1] L. A. Bokut, Y. Chen and Q. Mo, Gröbner–Shirshov bases for semirings, *J. Algebra* **385** (2013) 47–63.

[2] W. E. Clark, W. C. Holland and G. J. Székely, Decompositions in discrete semigroups, *Studia Sc. Math. Hungarica* **34** (1998) 15–23.

[3] M. Delgado, J. C. Rosales and P. A. García-Sánchez, Numerical semigroups problem list, *CIM Bull.* **33** (2013) 15–26.

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

[5] P. A. García-Sánchez, Numerical semigroups mini-course, http://www.ugr.es/∼pedro/minicurso-porto.pdf.

[6] J. S. Golan, *Semirings and Their Applications* (Kluwer Academic Publishers, Dordrecht, 1999).

[7] J. S. Golan, *Semirings and Affine Equations Over Them: Theory and Applications* (Kluwer Academic Publishers, Dordrecht, 2003).

[8] J. Gunawardena, An introduction to idempotency, in *Idempotency*, ed. J. Gunawardena (Cambridge University Press, Cambridge, 1998), pp. 1–49.

[9] U. Hebisch and H. J. Weinert, *Semirings: Algebraic Theory and Applications in Computer Science* (World Scientific Publishing, Singapore, 1998).

[10] J. Ježek, V. Kala and T. Kepka, Finitely generated algebraic structures with various divisibility conditions, *Forum Math.* **24**(2) (2012) 379–397.

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

[12] V. Kala, T. Kepka and M. Korbelář, Notes on commutative parasemifields, *Comment. Math. Univ. Carolin.* **50**(4) (2009) 521–533.

[13] T. Kepka and M. Korbelář, Conjectures on additively divisible commutative semirings, to appear in *Math. Slovaca*.

[14] F. Otto and O. Sokratova, Reduction relations for monoid semirings, *J. Symbolic Comput.* **37** (2004) 343–376.

[15] J. C. Rosales and P. A. García-Sánchez, *Numerical Semigroups*, Developments in Mathematics, Vol. 20 (Springer, 2009).

[16] T. Tamura, Minimal commutative divisible semigroups, *Bull. Amer. Math. Soc.* **69** (1963) 713–716.

[17] J. Zumbrägel, Classification of finite congruence-simple semirings with zero, *J. Algebra Appl.* **7**(4) (2008) 363–377.

Semigroup Forum (2017) 95:293–302
DOI 10.1007/s00233-016-9827-4

RESEARCH ARTICLE

Torsion and divisibility in finitely generated commutative semirings

Miroslav Korbelář[1,2]

Received: 30 September 2015 / Accepted: 13 September 2016 / Published online: 4 October 2016

Abstract It is conjectured that (additive) divisibility is equivalent to (additive) idempotency in a finitely generated commutative semiring S. In this paper we extend this conjecture to weaker forms of these properties—torsion and almost-divisibility (an element $a \in S$ is called *almost-divisible in* S if there is $b \in \mathbb{N} \cdot a$ such that b is divisible in S by infinitely many primes). We show that a one-generated semiring is almost-divisible if and only if it is torsion. In the case of a free commutative semiring $F(X)$ we characterize those elements $f \in F(X)$ such that for every epimorphism π of $F(X)$ torsion and almost-divisibility of $\pi(f)$ are equivalent in $\pi(F(X))$.

Keywords Commutative semiring · Divisible semigroup · Idempotent · Torsion

1 Introduction

Throughout the paper we assume that all algebraic structures (semigroups, monoids, semirings, groups and rings) are commutative.

In the theory of abelian groups, divisibility is one of the key notions [2–4], since injective modules are just all divisible groups. While a non-trivial divisible group can not be finitely generated, an abelian group A which is divisible with respect to some

Communicated by László Márki.

Miroslav Korbelář
miroslav.korbelar@gmail.com

[1] Department of Mathematics, Faculty of Electrical Engineering, Czech Technical University in Prague, Technická 2, 166 27 Praha 6, Czech Republic

[2] Department of Mathematics and Statistics, Faculty of Science, Masaryk University, Kotlářská 2, 611 37 Brno, Czech Republic

integer $k \geq 2$ might be non-trivial and finitely generated. Such a group A has to be finite and, therefore, divisible with respect to infinitely many prime numbers.

Similarly, a finitely generated ring R with divisible additive group $(R, +)$ has to be trivial, but there are non-trivial rings—e.g. the polynomial ring $\mathbb{Z}_2[x]$—which are finitely generated and the additive group $(R, +)$ is divisible only with respect to *almost all* prime numbers. Moreover, such a ring R always has to be torsion.

Our main intention is to generalize similar notions to semirings. In [9] it was conjectured that a finitely generated semiring with divisible additive part has to be idempotent (see 2.1 for all the necessary definitions). This hypothesis was motivated by the classification of simple semirings in [1] and was confirmed for the one-generated case in [10]. Under the additional assumption that the multiplicative part of the semiring is a group, this was proved for the at most two-generated case in [6] and [7].

In this paper we introduce the notion of almost-divisibility (see 2.1), which produces the following diagram:

$$\begin{tikzcd}
\text{idempotency} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{divisibility} \arrow[d, Rightarrow] \\
\text{torsion} \arrow[r, Rightarrow] & \text{almost-divisibility.}
\end{tikzcd}$$

We will study these properties in the frame of *additive* semigroups of finitely generated semirings. To the author's best knowledge, this is the first work on an equivalence between torsion and some sort of divisibility (even in the case of rings).

Additive parts of even one-generated semirings behave very wildly in general, as they may contain an arbitrary countable (commutative) semigroup, e.g. $(\mathbb{Q}, +)$ or the Prüfer group $\mathbb{Z}_{p^\infty}$ (see [10] for the detailed construction). On the other hand, additive groups of finitely generated rings are much more restricted (e.g. the only divisible subgroups they may contain are trivial).

Despite this contrast between rings and semirings, we find, surprisingly, for both structures similar theorems characterizing torsion elements via almost-divisibility (Theorems 4.4 and 5.1). This description is made in terms of free semirings and is of a "point-wise" nature. However, such an analogy turns out to be valid for special elements in one-generated semirings only (Theorem 5.2). Therefore we suggest a new conjecture of "global" character for finitely generated semirings (Conjecture 5.4):

Every almost-divisible finitely generated semiring has to be torsion.

This new hypothesis seems to be more plausible and extends naturally the result obtained in [10]. We confirm it for the one-generated case as well (Theorem 5.5).

Finally, let us point out that we substantially simplify the approach in [10], which uses rewriting of polynomials and the proof there is very long and technical. Simplicity of the main part of the proof in this paper (Theorem 4.4; the key Lemmas 4.1 and 4.3) is based on a special choice of a partial semigroup in Definition 2.1. To prove our assertions we use Laurent polynomials which help us to deal with the case when it is not possible to factor out common monomials from polynomial expressions on both sides of equalities. Such an approach consequently allows to involve naturally the methods from ring theory and results on finitely generated semigroups to prove our main goal on semirings.

2 Preliminaries

By a (commutative) *semiring* we mean a non-empty set equipped with two commutative and associative binary operations, an addition and a multiplication, such that the multiplication distributes over the addition. No constants, like additively and/or multiplicatively neutral elements, will be required and since all the investigated properties of semirings will be related to the additive semigroup only, we will usually omit the word *additively* which would stress this fact (e.g. we say "divisible" instead of "additively divisible").

We will use the usual notation: $\mathbb{N}$ ($\mathbb{N}_0$, resp.) for the semiring of positive (non-negative, resp.) integers, $\mathbb{Z}$ for the ring of integers, $\mathbb{Z}^-$ for the set of negative integers and $\mathbb{Q}$ for the ring of rational numbers.

Definition 2.1 Let $(A, +)$ be a commutative semigroup. For an element $a \in A$ and $k \in \mathbb{N}$ let $k \cdot a = a + \cdots + a$ be the k-fold sum of a. Set $\mathbb{N} \cdot a = \{\ell \cdot a | \; \ell \in \mathbb{N}\}$.

Let $\emptyset \neq M \subseteq \mathbb{N}$. An element $a \in A$ is called

- *torsion* $\Leftrightarrow |\mathbb{N} \cdot a| < \infty$.
- *idempotent* $\Leftrightarrow a + a = a$.
- *M-divisible (in A)* $\Leftrightarrow (\forall n \in M)(\exists c \in A)\; a = n \cdot c$.
- *divisible (in A)* $\Leftrightarrow$ a is $\mathbb{N}$-divisible (in A).
- *almost-divisible (in A)* $\Leftrightarrow$ there is $b \in \mathbb{N} \cdot a$ such that b is P-divisible (in A) for some infinite set of prime numbers P.

In the case of a semiring $(S, +, \cdot)$ we use the same notions for an element $a \in S$ with respect to the semigroup $(S, +)$. Consequently, we assign such a notion to the semiring S itself if and only if every element of S is so.

Further, for $n \geq 1$, we denote by $F(x_1, \ldots, x_n)$ the free commutative semiring with the basis $\{x_1, \ldots, x_n\}$ (i.e., $F(x_1, \ldots, x_n)$ consists of all non-zero polynomials over variables $\{x_1, \ldots, x_n\}$ which have non-negative integer coefficients and do not contain a constant term).

For a semiring $(S, +, \cdot)$ we always consider the natural pre-order $\leq_S$ on S defined as

$$a \leq_S b \;\Leftrightarrow\; a = b \text{ or } (\exists c \in S)\; a + c = b$$

for $a, b \in S$. This pre-order is compatible with multiplication and addition and depends on the choice of the semiring (e.g. $2 \not\leq_{\mathbb{N}} 1$ in $(\mathbb{N}, +, \cdot)$ but $2 \leq_{\mathbb{Z}} 1$ in $(\mathbb{Z}, +, \cdot)$).

In the sequel we will work with partial subsemigroups of $(\mathbb{Z}, +)$ (a set $\emptyset \neq A \subseteq \mathbb{Z}$ is a *partial subsemigroup* of $(\mathbb{Z}, +)$ if there is a relation $D \subseteq A \times A$ such that for every $(a, b) \in D$ we have $a + b \in A$, see [5]). For the sake of completeness we will prove a basic property of a special type of such partial semigroups.

Theorem 2.2 *(i) Every subsemigroup A of $(\mathbb{N}_0, +)$ is finitely generated and there is $n \in \mathbb{N}_0$ such that $d \cdot (n + \mathbb{N}_0) \subseteq A \subseteq d \cdot \mathbb{N}_0$, where $d = \gcd(A) \in \mathbb{N}_0$.*

(ii) Let A be a partial subsemigroup of $(\mathbb{Z}, +)$ such that for every $\alpha, \beta \in A$ we have $\alpha + \beta \in A$ if $\alpha \geq 0$.

If $A \cap \mathbb{Z}^- \neq \emptyset \neq A \cap \mathbb{N}$ then either $A = d \cdot \mathbb{Z}$ or $A = d \cdot (n_0 + \mathbb{N}_0)$ for some $n_0 \in \mathbb{Z}^-$, where $d = \gcd(A) \in \mathbb{N}_0$.

Proof (i) See [12, Chap. 1, Sect. 2].

(ii) Let $d^+ = \min(A \cap \mathbb{N}) > 0$ and $d^- = -\max(A \cap \mathbb{Z}^-) > 0$. Then $d^+ + (-d^-) \in A$ and $-d^- < -d^- + d^+ < d^+$. Hence $d^- = d^+ (= d_0)$ and $\{-d_0, 0, d_0\} \subseteq A$.

Let $a \in A \cap \mathbb{N}$. Then there are $k, r \in \mathbb{N}_0$ with $0 \leq r < d_0$ such that $a = d_0 k + r$. Now, by iteration argument, $0 \leq a + i(-d_0) \in A$ for every $i = 1, \ldots, k$. Thus $0 \leq r = a - kd_0 \in A$ and, consequently, $r = 0$ by the choice of d^+. Hence $A \cap \mathbb{N} = d_0 \cdot \mathbb{N}$.

Let $-b \in A \cap \mathbb{Z}^-$. Then there are $\ell, s \in \mathbb{N}_0$ with $0 \leq s < d_0$ such that $b = d_0 \ell + s$. Hence $0 \leq d_0 - s = d_0(\ell + 1) + (-b) \in A$ and, consequently, $s = 0$ by the choice of d^+. Thus $b = d_0 \ell$ and $-d_0 i = d_0(\ell - i) + (-b) \in A$ for every $i = 1, \ldots, \ell$.

Therefore $d_0 = \gcd(A)$ and either $A = d_0 \cdot \mathbb{Z}$ or $A = d_0 \cdot (n_0 + \mathbb{N}_0)$ for some $n_0 \in \mathbb{Z}^-$. □

The following definition is crucial for our next steps.

Definition 2.3 Let S be a commutative semiring. For $w \in S$ and $k, n \in \mathbb{N}$, put

$$^k\Pi_{w,n}(S) := \{\alpha \in \mathbb{Z} | \; n + \alpha > 0 \; \& \; k \cdot w^{n+\alpha} \leq_S k \cdot w^n\}.$$

This is a generalization of the submonoid $\Pi_w(S) = \{\alpha \in \mathbb{N}_0 | \; w^\alpha \leq_S 1_S\}$ of $(\mathbb{N}_0, +)$ introduced in [10].

Proposition 2.4 *Let S be a commutative semiring, $w \in S$ and $n, k \in \mathbb{N}$. Let $A = {}^k\Pi_{w,n}(S)$. Then $(A, +)$ is a partial submonoid of $(\mathbb{Z}, +)$ such that for every $\alpha, \beta \in A$ we have $\alpha + \beta \in A$ if $\alpha \geq 0$.*

If $A \cap \mathbb{N} \neq \emptyset$, then there is $n_0 \in \mathbb{Z}$ such that $d \cdot (n_0 + \mathbb{N}_0) \subseteq A \subseteq d \cdot \mathbb{Z}$, where $d = \gcd(A) \in \mathbb{N}$. If, moreover, $A \cap \mathbb{Z}^- \neq \emptyset$ then $n_0 \in \mathbb{Z}$ can be chosen such that $A = d \cdot (n_0 + \mathbb{N}_0)$.

Proof Let $\alpha, \beta \in A$ and $\alpha \geq 0$. Then $k \cdot w^{n+\alpha} \leq_S k \cdot w^n$ and $k \cdot w^{n+\beta} \leq_S k \cdot w^n$. Since $\alpha \geq 0$, we have $k \cdot w^{n+\alpha+\beta} \leq_S k \cdot w^{n+\alpha}$ and therefore $k \cdot w^{n+\alpha+\beta} \leq_S k \cdot w^{n+\alpha} \leq_S k \cdot w^n$. Thus $\alpha + \beta \in A$. The rest follows immediately from 2.2. □

3 Torsion and divisibility in rings and semigroups

First, we derive auxiliary results for finitely generated semigroups and show that almost-divisibility is the right notion that is equivalent to torsion in finitely generated rings.

Lemma 3.1 *[10, Proposition 5.1] Let $(A, +)$ be a finitely generated commutative semigroup. Let $M \subseteq \mathbb{N}$ be an infinite set and $\{v_m | \; m \in M\} \subseteq A$. Then there are $\ell \in \mathbb{N}$, $m_1, \ldots, m_\ell \in M$ and $c_{1,j}, \ldots, c_{\ell,j} \in \mathbb{N}$, $j = 0, 1$ such that $\sum_{i=1}^{\ell} c_{i,0} m_i \cdot v_{m_i} = \sum_{i=1}^{\ell} c_{i,1} m_i \cdot v_{m_i}$ and $\sum_{i=1}^{\ell} c_{i,0} \neq \sum_{i=1}^{\ell} c_{i,1}$.*

Proposition 3.2 *Let $(A, +)$ be a commutative monoid, $B \subseteq A$ be a finitely generated submonoid, $\mathcal{T}$ be the submonoid of all torsion elements of A.*

Let $u \in A$ and let $M \subseteq \mathbb{N}$ be an infinite set, $\{v_m \mid m \in M\} \subseteq B$ and $\{t_m \mid m \in M\} \subseteq \mathcal{T}$ be such that $u = mv_m + t_m$ for every $m \in M$. Then u is torsion.

Proof By 3.1, there are $\ell \in \mathbb{N}, m_1, \dots, m_\ell \in M$ and $c_{1,j}, \dots, c_{\ell,j} \in \mathbb{N}$, $j = 0, 1$ such that $v = \sum_{i=1}^{\ell} c_{i,0} m_i \cdot v_{m_i} = \sum_{i=1}^{\ell} c_{i,1} m_i \cdot v_{m_i}$ and $c_0 = \sum_{i=1}^{\ell} c_{i,0} \neq \sum_{i=1}^{\ell} c_{i,1} = c_1$.

Set $s_j = \sum_{i=1}^{\ell} c_{i,j} m_i \cdot t_{m_i} \in \mathcal{T}$ for $j = 0, 1$. Then $c_j \cdot u = \sum_{i=1}^{\ell} c_{i,j} u = \sum_{i=1}^{\ell} c_{i,j}(m_i v_{m_i} + t_{m_i}) = v + s_j$. Since $s_0, s_1 \in \mathcal{T}$, there is a common $k \in \mathbb{N}$ such that $ks_0 = 2ks_0$ and $ks_1 = 2ks_1$.

Now, $(kc_0 + kc_1) \cdot u = kv + ks_0 + kv + ks_1 = (2kv + 2ks_0) + ks_1 = 2kc_0 \cdot u + ks_1$. Finally, multiplying this equation by two, we get

$$\begin{aligned} 2k(c_0 + c_1) \cdot u &= 4kc_0 \cdot u + 2ks_1 = 2kc_0 \cdot u + (2kc_0 \cdot u + ks_1) \\ &= 2kc_0 \cdot u + (kc_0 + kc_1) \cdot u = k(3c_0 + c_1) \cdot u. \end{aligned}$$

Hence u is torsion since $2k(c_0 + c_1) \neq k(3c_0 + c_1)$. □

As an immediate consequence we obtain:

Theorem 3.3 *Let $(A, +)$ be a finitely generated commutative semigroup. The following are equivalent for $a \in A$:*

(i) *a is torsion.*
(ii) *$k \cdot a$ is M-divisible for some infinite set $M \subseteq \mathbb{N}$ and some $k \in \mathbb{N}$.*

Notice that if A is a finitely generated semigroup such that $A = k \cdot A$ for some $k \geq 2$, then A is M-divisible for $M = \{k^n \mid n \in \mathbb{N}\}$ and therefore torsion and finite by 3.3.

Rings now offer further equivalent descriptions of torsion compared to semigroups.

Theorem 3.4 *[8, 5.2] Let R be a finitely generated commutative ring with unity and let M be a finitely generated unitary R-module such that $pM = M$ for infinitely many prime numbers p. Then there is $n \in \mathbb{N}$ such that $nM = 0$.*

Theorem 3.5 *Let R be a finitely generated commutative ring. The following are equivalent for $a \in R$:*

(i) *a is torsion.*
(ii) *a is P-divisible for some infinite set of prime numbers $P \subseteq \mathbb{P}$.*
(iii) *$k \cdot a$ is divisible for some $k \in \mathbb{N}$.*
(iv) *a is almost-divisible.*

Proof The implications (i)⇒(iii) and (iii)⇒(iv) are easy.

(i)⇒(ii): Let a be torsion. Then there is $k \in \mathbb{N}$ such that $ka = 0$. Set $P = \{p \in \mathbb{P} \mid \gcd(p, k) = 1\}$. For $p \in P$ there are $i, j \in \mathbb{Z}$ such that $1 = ik + jp$, hence $a = ika + jpa = p \cdot ja$. Thus a is P-divisible.

(ii)⇒(i): We show that the set $I = \{x \in R \mid x \text{ is } P\text{-divisible}\}$ is a torsion group. Clearly, I is a non-zero ideal of R. The set $M = \{b \in R \mid (\exists n \in \mathbb{N})\ nb \in I\}$ is also an ideal of R and $I \subseteq M$. Since R is noetherian, M/I is a finitely generated R-module. Further, the group $(M/I, +)$ is torsion and for a set of generators of M/I we therefore have a common $n_0 \in \mathbb{N}$ such that $n_0 \cdot M/I = 0$.

Now, the set $\tilde{P} = \{p \in P \mid \gcd(n_0, p) = 1\}$ is infinite. We show that $M \subseteq pM$ for every $p \in \tilde{P}$. Let $b \in M$ and $p \in \tilde{P}$. Then there are $k, \ell \in \mathbb{Z}$ such that $1 = kn_0 + \ell p$. Hence $b = k(n_0 b) + p(\ell b)$. Since $n_0 b \in I$, there is $c \in R$ such that $pc = n_0 b \in I$. Therefore $c \in M$ and we have $b = p(kc + \ell b) \in pM$.

Finally, we have obtained that $pM = M$ for every $p \in \tilde{P}$. Clearly, M is a finitely generated unitary $\tilde{R}$-module with respect to some finitely generated commutative ring $\tilde{R}$ with unit. Hence M is a torsion group, by 3.4, as well as I.

(iv)⇒(i): Let $b = ka$ be P-divisible for some infinite set of prime numbers $P \subseteq \mathbb{P}$ and some $k \in \mathbb{N}$. Thus b is torsion, by the previously proved implication (ii)⇒(i). Hence a is torsion. □

4 Torsion and almost-divisibility in one-generated semirings

First, let us recall the notion of the *Grothendieck ring* $G(S)$ of a commutative semiring $(S, +, \cdot)$. It is constructed as follows (see e.g. [11]):

On the set $\tilde{S} = S \times S$ we define operations $\oplus$ and $\odot$ by

$$(a, b) \oplus (a', b') = (a + a', b + b') \ \text{ and } \ (a, b) \odot (a', b') = (aa' + bb', ab' + a'b)$$

and a relation $\approx$ by

$$(a, b) \approx (a', b') \ \Leftrightarrow \ (\exists t \in S)\ a + b' + t = a' + b + t$$

for every $a, a', b, b' \in S$. Now $\approx$ is a congruence on the semiring $(\tilde{S}, \oplus, \odot)$ and $G(S) = \tilde{S}_{/\approx}$ is a ring. We also have a semiring homomorphism $S \to G(S)$, defined by $a \mapsto (2a, a)_{/\approx}$ for $a \in S$.

We are now going to generalize Theorem 3.5 from rings to one-generated semirings (see 4.4). The key-point are the properties of ${}^{k}\Pi_{w,n}(S)$ formulated in Proposition 2.4.

Lemma 4.1 *Let S be a commutative semiring generated by $w \in S$. Let $n, k \in \mathbb{N}$ be such that $k \cdot w^n$ is P-divisible in S for some infinite set of prime numbers $P \subseteq \mathbb{P}$ and ${}^{k}\Pi_{w,n}(S) \cap \mathbb{N} \neq \emptyset$.*

Then there is a polynomial $f \in F(z)$ and $k_1, k_2, \ell_0 \in \mathbb{N}$ such that $k_1 \neq k_2$ and $k_1 w^{d\ell_0} + f(w^d) = k_2 w^{d\ell_0} + f(w^d)$, where $d = \gcd\left({}^{k}\Pi_{w,n}(S)\right)$.

Proof Let $L(z)$ denote the semiring of all non-zero Laurent polynomials over a variable z with non-negative integer coefficients and consider the free semiring $F(z)$ to be contained naturally in $L(z)$. Clearly, $L(z)$ is generated by $\{z, z^{-1}\}$. Set a relation $\equiv$ on $L = L(z)$ as follows:

For $g(z), h(z) \in L$ we put $g \equiv h$ if and only if there is $\ell \in \mathbb{N}$ such that $g(z)z^{\ell}, h(z)z^{\ell} \in F(z)$ and $g(w^d)w^{d\ell} = h(w^d)w^{d\ell}$. It is easy to check that $\equiv$ is a semiring congruence on L.

By 2.4, ${}^k\Pi_{w,n}(S) \subseteq d \cdot \mathbb{Z}$. Since $k \cdot w^n$ is P-divisible in S, for every $p \in P$ there is $f_p(z) \in L$ such that $f_p(z^d)z^n \in F(z)$ and $k \cdot w^n = p \cdot f_p(w^d)w^n$. Hence $k \equiv p \cdot f_p(z)$ and $k \cdot 1_{/\equiv}$ is a P-divisible element in the finitely generated semiring $L_{/\equiv}$. Let $\mathbf{u} \in G(L_{/\equiv})$ correspond to $1_{/\equiv} \in L_{/\equiv}$ in the finitely generated Grothendieck ring $G(L_{/\equiv})$. Then the element $k \cdot \mathbf{u} \in G(L_{/\equiv})$ is P-divisible. By 3.5, $\mathbf{u}$ is torsion and therefore, by the Grothedieck construction, there is a Laurent polynomial $f_0(z) \in L$ and $k_1, k_2 \in \mathbb{N}$, $k_1 \neq k_2$ such that $k_1 + f_0(z) \equiv k_2 + f_0(z)$. According to the definition of $\equiv$, there is $\ell_0 \in \mathbb{N}$ such that $f_0(z)z^{\ell_0} \in F(z)$ and $k_1 w^{d\ell_0} + f_0(w^d)w^{d\ell_0} = k_2 w^{d\ell_0} + f_0(w^d)w^{d\ell_0}$. Now, set $f(z) = f_0(z)z^{\ell_0}$ and we are done. □

Remark 4.2 Let S be a commutative semiring generated by $w \in S$ and let $n \in \mathbb{N}$.

(i) Let $k \in \mathbb{N}$. If $f \in F(x)$ is such that $\{\beta \in \mathbb{Z} | \ x^{\beta+n}$ is contained in $f(x)\} \subseteq {}^k\Pi_{w,n}(S)$ then there is $\ell \in \mathbb{N}$ such that $k \cdot f(w) \leq_S k\ell \cdot w^n$.

(ii) Set a relation $\sim_{w,n}$ on $(S,+)$ such that $a \sim_{w,n} b$ if and only if there is $j \in \mathbb{N}$ such that $a + jw^n = b + jw^n$. It is easy to check that $\sim_{w,n}$ is a congruence on the semigroup $(S,+)$.

Lemma 4.3 *Let $n, k \in \mathbb{N}$ and S be a commutative semiring generated by $w \in S$ such that ${}^k\Pi_{w,n}(S) \cap \mathbb{N} \neq \emptyset$. Further, let $\pi : (S,+) \to (S_{/\sim_{w,n}},+)$ be the natural semigroup epimorphism (see 4.2(ii)).*

If $k \cdot w^n$ is P-divisible in S for some infinite set of prime numbers $P \subseteq \mathbb{P}$, then there is $m_0 \in \mathbb{N}$ such that the element $\pi(w^{\alpha+n})$ is torsion in $\pi(S)$ for every $\alpha \in {}^k\Pi_{w,n}(S)$, $\alpha \geq m_0$.

Proof Set $d = \gcd\left({}^k\Pi_{w,n}(S)\right)$. By 4.1, there is a polynomial $f \in F(z)$ and $k_1, k_2, \ell_0 \in \mathbb{N}$ such that $k_1 \neq k_2$ and $k_1 w^{d\ell_0} + f(w^d) = k_2 w^{d\ell_0} + f(w^d)$. Further, by 2.4, there is $j_0 \in \mathbb{N}$ such that $d \cdot (j_0 + \mathbb{N}_0) \subseteq {}^k\Pi_{w,n}(S)$. Set $m_0 = d(j_0 + \ell_0)$ and let f be of the form $f(z) = \sum_{i \geq 0} a_i z^i$, where $a_i \in \mathbb{N}_0$.

Now, let $\alpha \in {}^k\Pi_{w,n}(S) \subseteq d \cdot \mathbb{Z}$ be such that $\alpha \geq m_0$. Then $\alpha = dj$ for some $j \geq j_0 + \ell_0$ and for every $i \in \mathbb{N}_0$ we therefore have $\alpha + d(i - \ell_0) = d(j - \ell_0 + i) \in d \cdot (j_0 + \mathbb{N}_0) \subseteq {}^k\Pi_{w,n}(S)$. Set $g(z) = f(z^d)z^{\alpha - d\ell_0 + n} = \sum_{i \geq 0} a_i z^{\alpha + d(i-\ell_0)+n} \in F(z)$. Obviously, we have $\{\beta \in \mathbb{Z} | \ z^{\beta+n}$ is contained in $g(z)\} \subseteq {}^k\Pi_{w,n}(S)$ and hence, by 4.2(i), there is $\ell \in \mathbb{N}$ such that

$$k \cdot f(w^d)w^{\alpha - d\ell_0 + n} = k \cdot g(w) \leq_S k\ell \cdot w^n.$$

Therefore there is $u \in S$ such that $u + k \cdot f(w^d)w^{\alpha - d\ell_0 + n} = k(\ell + 1) \cdot w^n$.

Finally, multiplying the equality $k_1 w^{d\ell_0} + f(w^d) = k_2 w^{d\ell_0} + f(w^d)$ by the element $k \cdot w^{\alpha - d\ell_0 + n}$ and then adding the element u to both sides we get

$$kk_1 w^{\alpha+n} + k(\ell+1) \cdot w^n = kk_2 w^{\alpha+n} + k(\ell+1) \cdot w^n$$

where $kk_1 \neq kk_2$. Therefore $\pi(w^{\alpha+n})$ is a torsion element of the semigroup $\pi(S) = S_{/\sim_{w,n}}$ for every $\alpha \in {}^k\Pi_{w,n}(S)$ such that $\alpha \geq m_0$. □

The semiring version of Theorem 3.5 now reads as follows:

Theorem 4.4 *Let S be a semiring generated by $w \in S$. The following are equivalent for an element $v \in \bigcup_{n\in\mathbb{N}} \mathbb{N}w^n$:*

(i) v is torsion.
(ii) $k \cdot v$ is divisible for some $k \in \mathbb{N}$.
(iii) v is almost-divisible.

Proof The implications (i)⇒(ii) and (ii)⇒(iii) are obvious.

(iii)⇒(i): Let $v = c \cdot w^n$ for some $c \in \mathbb{N}$ and $n \in \mathbb{N}$. Let $k \in \mathbb{N}$ be such that $k \cdot v$ is P-divisible for some infinite set of prime numbers $P \subseteq \mathbb{P}$.

First, assume that ${}^{kc}\Pi_{w,n}(S) \cap \mathbb{N} = \emptyset$. In this case $k \cdot cw^n$ is a P-divisible element of a subsemigroup A of $(S, +)$ which is generated by the elements $w, w^2, \ldots, w^n$. Hence $v = cw^n$ is torsion, by 3.3.

Now, let ${}^{kc}\Pi_{w,n}(S) \cap \mathbb{N} \neq \emptyset$ and let $\pi : (S, +) \to (S_{/\sim_{w,n}}, +)$ be the natural semigroup epimorphism [see 4.2(ii)]. By 4.3, there is $m_0 \in \mathbb{N}$ such that for every $\alpha \in {}^{kc}\Pi_{w,n}(S)$, $\alpha \geq m_0$ is $\pi(w^{\alpha+n})$ a torsion element of $\pi(S)$.

Further, let A be the monoid obtained from $\pi(S)$ (i.e., we adjoin a unit element 0 to $\pi(S)$ if there is none). Let B be the submonoid of A generated by the finite set $\{\pi(w^{\alpha+n})|\ \alpha \in {}^{kc}\Pi_{w,n}(S)\ \&\ \alpha < m_0\}$. Similarly, let C be the submonoid of A generated by the set $\{\pi(w^{\alpha+n})|\ \alpha \in {}^{kc}\Pi_{w,n}(S)\ \&\ \alpha \geq m_0\}$. Clearly, B is finitely generated and C is torsion. Since $kc \cdot w^n$ is P-divisible, for every $p \in P$ there are $r_p \in B$ and $s_p \in C$ such that $kc \cdot \pi(w^n) = p(r_p + s_p)$. Therefore, by 3.2, $kc \cdot \pi(w^n)$ is a torsion element of $\pi(S)$. Thus there are $j, k_1, k_2 \in \mathbb{N}$ such that $k_1 \neq k_2$ and $k_1kc \cdot w^n + j \cdot w^n = k_2kc \cdot w^n + j \cdot w^n$. Hence w^n and $v = c \cdot w^n$ are torsion elements. □

5 Conclusion and further questions

Compared to rings, Theorem 4.4 provides information about a quite special kind of elements in one-generated semirings only. But as Theorem 5.2 shows, it is not possible to expect such a description in full generality (i.e., for other kinds of elements or for cases of several generators).

Before we formulate the main result, let us recall a theorem from [10] (here $F(x_1, \ldots, x_n)$ is a free commutative semiring with basis $\{x_1, \ldots, x_n\}$):

Theorem 5.1 *[10, Theorem 6.1] Let $(A, +)$ be an at most countable commutative semigroup, $n \in \mathbb{N}$, $a \in A$ and $f \in F(x_1, \ldots, x_n)$.*

If either $n \geq 2$ or f contains at least two different monomials, then there is a commutative semiring S generated by a set $\{w_1, \ldots, w_n\} \subseteq S$ such that $(A, +)$ is a subsemigroup of $(S, +)$ and $f(w_1, \ldots, w_n) = a$.

Now, we can summarize our results as follows:

Theorem 5.2 *Let $n \in \mathbb{N}$. The following are equivalent for $f \in F(x_1, \ldots, x_n)$:*

(i) *For every semiring S and every semiring epimorphism $\varphi : F(x_1, \ldots, x_n) \to S$, the element $\varphi(f)$ is torsion if and only if it is almost-divisible in S.*
(ii) *$n = 1$ and $f = k \cdot x_1^m$ for some $k, m \in \mathbb{N}$.*

Proof (i)⇒(ii): Let $n \geq 2$ or let f contain at least two different monomials. Choose some $a \in \mathbb{Q}^+$. By 5.1, there is a semiring S and a semiring epimorphism $\varphi : F(x_1, \dots, x_n) \to S$ such that $(\mathbb{Q}^+, +)$ is a subsemigroup of $(S, +)$ and $\varphi(f) = a \in S$. Since $\ell a \in \mathbb{Q}^+$ is divisible and torsion-free for every $\ell \in \mathbb{N}$, we get that $\varphi(f)$ is almost-divisible but not torsion.

(ii)⇒(i): Follows immediately from 4.4. □

Remark 5.3 (i) In view of Theorem 3.3 (4.4, resp.) it seems to be likely that if an element is divisible by infinitely many numbers (primes, resp.), then not only it is torsion, but it should generate a finite *group*.

(ii) Assume now that, for a semigroup A and a given element $a \in A$, the following conditions hold:

- The set $F_a = \{x \in A | \, (\exists n \in \mathbb{N}) \; a = nx\}$ of all possible fractions of a in A is contained in some *finitely generated* subsemigroup of A.
- The element a is divisible in A by an *infinite set of integers*.

Under these assumptions, a is torsion, by Theorem 3.3.

On the other hand, in a semiring S generated by $w \in S$, divisibility of an element $a \in \bigcup_{n \in \mathbb{N}} \mathbb{N}w^n \subseteq S$ by *infinitely many primes* forces torsion as well (see Theorem 4.4). Therefore it is natural to ask whether or not this is caused by some restrictions on the set F_a for such an element $a \in S$.

In particular, we ask whether, for $a \in \bigcup_{n \in \mathbb{N}} \mathbb{N}w^n \subseteq S$, the set F_a is contained in some *finitely generated* subsemigroup of $(S, +)$ (or whether at least a “substantial” part of F_a has this property).

Finally, by Theorem 5.2, torsion and almost-divisibility are not generally equivalent for a single element in a finitely generated semiring. However, when we consider all elements at the same time, the situation may be different and the following might be true:

Conjecture 5.4 *For a finitely generated commutative semiring S, the following are equivalent:*

- *Every element of S is torsion.*
- *Every element of S is almost-divisible.*

This conjecture is now confirmed for the one-generated case, by 4.4:

Theorem 5.5 *Every one-generated almost-divisible semiring is torsion.*

Acknowledgements The author was supported by the Czech Science Foundation (GAČR) by grant GP13-29835P. Also, I would like to express my thanks to Jan Šaroch (Department of Algebra, Charles University in Prague) for his valuable suggestions and comments.

References

1. El Bashir, R., Hurt, J., Jančařík, A., Kepka, T.: Simple commutative semirings. J. Algebra **236**, 277–306 (2001)
2. Fuchs, L.: Abelian Groups. Budapest/Pergamon Press, Akadémiai Kiadó (1960)

3. Fuchs, L.: Infinite Abelian Groups, Pure and Applied Mathematics, vol. 1. Academic Press, New York (1970)
4. Fuchs, L., Salce, L.: Modules over Non-Noetherian Domains. In: Mathematical Surveys and Monographs, vol. 84. American Mathematical Society, Providence (2001)
5. Grillet, P.A.: Commutative Semigroups. Kluwer Academic Publishers, Dordrecht (2001)
6. Ježek, J., Kala, V., Kepka, T.: Finitely generated algebraic structures with various divisibility conditions. Forum Math. **24**(2), 379–397 (2012)
7. Kala, V., Kepka, T., Korbelář, M.: Notes on commutative parasemifields. Comment. Math. Univ. Carol. **50**, 521–533 (2009)
8. Kechlibar, M., Kepka, T., Kortelainen, J.: A note on finitely generated commutative rings. Acta Univ. Carol. Math. Phys. **46**(1), 101–105 (2005)
9. Kepka, T., Korbelář, M.: Conjectures on additively divisible commutative semirings. Math. Slovaca (arXiv version: https://arxiv.org/pdf/1401.2836)
10. Korbelář, M., Landsmann, G.: One-generated semirings and additive divisibility. J. Algebra Appl. **16**(1), 22 (2017). doi:10.1142/S0219498817500384
11. May, J.P.: A Concise Course in Algebraic Topology, 2nd edn. University of Chicago Press, Chicago (1999)
12. Rosales, J.C., García-Sánchez, P.A.: Numerical Semigroups. Springer, New York (2009)

Journal of Algebra and Its Applications
Vol. 17, No. 4 (2018) 1850071 (10 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0219498818500718

Divisibility and groups in one-generated semirings

Miroslav Korbelář
Department of Mathematics, Faculty of Electrical Engineering
Czech Technical University in Prague, Technická 2
166 27 Prague, Czech Republic
miroslav.korbelar@gmail.com

Received 4 July 2015
Accepted 29 March 2017
Published 5 May 2017

Communicated by I. Shestakov

Let $(S, +, \cdot)$ be a semiring generated by one element. Let us denote this element by $w \in S$ and let $g(x) \in x \cdot \mathbb{N}[x]$ be a polynomial. It has been proved that if $g(x)$ contains at least two different monomials, then the elements of the form $g(w)$ may possibly be contained in any countable commutative semigroup. In particular, divisibility of such elements does not imply their torsion. Let, on the other hand, $g(x)$ consist of a single monomial (i.e. $g(x) = kx^n$, where $k, n \in \mathbb{N}$). We show that in this case, the divisibility of $g(w)$ by infinitely many primes implies that $g(w)$ generates a group within $(S, +)$. Further, an element $a \in S$ is called an m-fraction of an element $z \in S$ if $m \in \mathbb{N}$ and $z = m \cdot a$. We prove that "almost every" m-fraction of w^n can be expressed as $f(w)$ for some polynomial $f \in x \cdot \mathbb{N}[x]$ of degree at most n.

Keywords: Commutative semiring; divisible semigroup; idempotent; inverse semigroup.

Mathematics Subject Classification: 16Y60, 20M14, 20M18, 13C12

In this paper, a (commutative) *semiring* $(S, +, \cdot)$ is a non-empty set equipped with two commutative and associative binary operations, an addition and a multiplication, such that the multiplication distributes over the addition. We denote by $\langle D\rangle^+$ the subsemigroup of $(S, +)$ generated by a non-empty subset D of S. In particular, for $a \in S$ we have $\langle a\rangle^+ = \{a, 2a, \cdots\}$.

Let M be a non-empty subset of positive integers $\mathbb{N}$. We say that an element $a \in S$ is

- *torsion* $\Leftrightarrow$ $\langle a\rangle^+$ is finite,
- *M-divisible (in S)* $\Leftrightarrow$ for every $m \in M$ there is $b \in S$ such that $a = m \cdot b$,
- *divisible (in S)* $\Leftrightarrow$ a is $\mathbb{N}$-divisible (in S),
- *almost divisible (in S)* $\Leftrightarrow$ there is an element $b \in \langle a\rangle^+$ that is P-divisible (in S) for some infinite set P of prime numbers.

We assign such notions to the entire semiring S when every element of S is so. We adopt all the semiring notions to a commutative semigroup, too.

As an analogy to an mth root of an element for $m \in \mathbb{N}$, we say that an element $a \in S$ is an *m-fraction* of an element $z \in S$ if $z = m \cdot a$. Finally, let us denote by

$$\left(\frac{X}{M}\right)_S = \{a \in S \,|\, (\exists x \in X)(\exists m \in M)\ x = ma\}$$

the set of *all M-fractions of a non-empty subset X in a commutative semiring S*, where M is a non-empty subset of positive integers.

One-generated semirings may possibly contain any countable commutative semigroup $(A, +)$ in their additive semigroups [8]. Moreover, let $f(x) \in x \cdot \mathbb{N}[x]$ be a polynomial containing at least two different monomials and let $a \in A$. Then there is a semiring S generated by $w \in S$ such that $(A, +)$ is a subsemigroup of $(S, +)$ and $a = f(w)$ [8, Theorem 6.1]. In particular, divisibility of such elements does not imply their torsion.

The only terms in the free semiring $x \cdot \mathbb{N}[x]$ that cannot be mapped arbitrarily in this way are the polynomials $f(x) = kx^n$, where $k, n \in \mathbb{N}$. In this paper, we investigate their properties related to the divisibility in more detail. The first steps were made in [7], where it was shown that the almost divisibility implies the torsion of elements kw^n.

Theorem A ([7, Theorem 3.4]). *Let S be a semiring generated by $w \in S$. Then for every $z \in \bigcup_{n\in\mathbb{N}} \langle w^n \rangle^+$ the following conditions are equivalent*:

(i) *the semigroup $\langle z \rangle^+$ is finite*,
(ii) *z is almost divisible in S.*

In [7], it was also conjectured that in a finitely generated commutative semiring the almost divisibility of *all* elements shall imply their torsion. A particular version of this conjecture can be stated as follows:

Conjecture I. *Let S be a finitely generated commutative semiring. Then the following conditions are equivalent*:

(i) *For every element $z \in S$ the semigroup $\langle z \rangle^+$ is a group.*
(ii) *Every element $z \in S$ is P-divisible in S by for some infinite set P of primes.*

Note that the condition (i) in Conjecture I can be expressed in a form that the semigroup $(S, +)$ is Clifford and torsion. Let us recall that a semigroup is Clifford if it is completely regular and inverse (see e.g. the monograph by Grillet [3]). Inverse semigroups possessing 2-divisibility were also recently studied by Araújo and Kinyon [1]. It should also be observed that in a weaker form of Conjecture I, the first condition of the equivalence is replaced with idempotency and the second condition is replaced with $\mathbb{N}$-divisibility. Thus, this note can be viewed as a contribution to the study of idempotent semirings at large (see e.g. [5, 6] and [9]).

The validity of Conjecture I can easily be inferred from the validity of the original hypothesis (there is a common bound on all orders of all elements). However, as it was noticed above, such a conjecture requires that *all* elements share a given property (the divisibility by infinitely many prime numbers). In this paper, we investigate the case when only a *single* element has this property. In particular, we are going to establish the following result:

Theorem 0.1. *Let S be a semiring generated by $w \in S$. Then for all $z \in \bigcup_{n\in\mathbb{N}}\langle w^n\rangle^+$ the following two conditions are equivalent*:

(i) *the semigroup $\langle z\rangle^+$ is a group,*
(ii) *z is P-divisible in S for some infinite set P of primes.*

In particular, for all $z \in \bigcup_{n\in\mathbb{N}}\langle w^n\rangle^+$ the following two conditions are equivalent:

(iii) *z is idempotent,*
(iv) *z is divisible in S.*

Theorem 0.1 is a particular case of Theorem A. It confirms the natural expectation that if P-divisibility is related to an element z itself (and not only to some of its multiples) then the cyclic semigroup $\langle z\rangle^+$ becomes a group. It is also an extension of the following theorem by Clark, Holland and Székely [2]:

Theorem B ([2, Theorem 2.5(i)]). *Every divisible element in a finitely generated commutative semigroup is idempotent.*

However, the proof of Theorem 0.1 is not as straightforward as it may seem. The main problem is the case when for the given $k, n \in \mathbb{N}$ there are polynomials $f_m(x)$ of arbitrary large degrees such that $kw^n = m \cdot f_m(w)$ and when the polynomials f_m also contain some monomials of degrees less than n.

Further, we also generalize another theorem that is originally formulated in [2].

Theorem C ([2, Theorem 2.7]). *If $(A, +)$ is a residually finite semigroup then every divisible element of A is idempotent.*

Our generalization reads as follows:

Theorem 0.2. *Let $(A, +)$ be a residually finite semigroup and $z \in A$. Then the following two conditions are equivalent*:

(i) *the semigroup $\langle z\rangle^+$ is a group,*
(ii) *z is M-divisible in A for some infinite set M of positive integers.*

In particular, this is also true if A is a finitely generated commutative semigroup (*such a semigroup is residually finite by a well-known theorem of Mal'cev* [10]).

To continue, in [8], it was proved that there are restrictions on the set of fractions of a generator of a semiring. The result was as follows:

Theorem D ([8, Theorem 4.2]). *Let S be a semiring generated by $w \in S$ and let S have a unity 1_S. Then there are $k \in \mathbb{N}$ and $i \in \mathbb{N}$ such that*

$$\left(\frac{w}{M}\right)_S \subseteq \langle w, w^2, \ldots, w^i \rangle^+,$$

where $M = \{m \in \mathbb{N} \mid \gcd(m,k) = 1\}$.

We extend and improve on this result to *all* powers of the generator $w \in S$ in the following way.

Theorem 0.3. *Let S be a semiring generated by $w \in S$. For every $n \in \mathbb{N}$ there is $k \in \mathbb{N}$ such that*

$$\left(\frac{w^n}{M}\right)_S \subseteq \langle w, w^2, \ldots, w^n \rangle^+,$$

where $M = \{m \in \mathbb{N} \mid \gcd(m,k) = 1\}$. In particular, $\left(\frac{w}{M}\right)_S \subseteq \langle w \rangle^+$.

This result shows that fractions of elements w^n are surprisingly restricted in the sense that almost every fraction of w^n can be expressed as $f(w)$ for some polynomial $f \in x \cdot \mathbb{N}[x]$ of degree at most n. Here, the expression *almost every* means that there is a finite set of primes P and the given statement is true for every number that is not divisible by any prime from P. Exercising some more effort, it can be shown that in Theorem 0.3 there is a universal $k \in \mathbb{N}$ for all $n \in \mathbb{N}$.

Finally, we provide a far stronger version of Theorem 0.3 in the case of commutative rings:

Theorem 0.4. *Let R be a finitely generated commutative ring and G be a finitely generated subgroup of $(R,+)$. Then there is $k \in \mathbb{N}$ such that $\left(\frac{G}{M}\right)_R \subseteq G$, where $M = \{m \in \mathbb{N} \mid \gcd(m,k) = 1\}$.*

Remark 0.5. (i) Note (Results 1.1(i)) that if $z \in S$ is M-divisible (in S), M is infinite and $\left(\frac{z}{M}\right)_S$ is contained in a finitely generated subsemigroup of $(S,+)$, then z is torsion. Therefore, Theorem A follows from Theorem 0.3 in the special case when $z = w^n$. In this case, we obtain henceforth a better insight into the structure of such a semiring.

(ii) Unlike Theorem 0.1, Theorem 0.3 cannot be extended to all elements of the set $\bigcup_{n\in\mathbb{N}} \langle w^n \rangle^+$. Indeed, consider a semiring $(S,+,\cdot)$ with a multiplicatively absorbing element 0 such that the semigroup $(S \backslash \{0\}, \cdot)$ is isomorphic to $(\mathbb{N},+)$. Let $w \in S\backslash\{0\}$ be the (unique) generator of this semigroup. Let us define the additive operation by setting $a + b = 0$ for all $a, b \in S$. Clearly, S is a semiring generated by w. For every non-empty set M of $\mathbb{N}\backslash\{1\}$ and for all $n, k \in \mathbb{N}$, $k \geq 2$ we obtain $z := kw^n = 0$ and $\left(\frac{z}{M}\right)_S = S$. Hence, $\left(\frac{z}{M}\right)_S$ is not contained in any finitely generated semigroup of $(S,+)$. Therefore, there is no upper bound on the degrees of polynomials expressing elements from the set $\left(\frac{z}{M}\right)_S$.

(iii) In Theorem 0.3, we do not require $\left(\frac{w^n}{M}\right)_S \subseteq \langle w^n\rangle^+$ for $n \geq 2$. Indeed, assume a semiring $(S, +, \cdot)$ with a multiplicatively absorbing element 0 such that the semigroup $(S, \cdot)$ has a presentation $\langle w \,|\, w^{n+1} = 0\rangle$. The additive operation is defined by setting $a + b = w^n$ for all $a, b \in S\backslash\{0\}$ and $c + 0 = 0 + c = c$ for every $c \in S$. Clearly, S is a finite semiring generated by the element w and for every non-empty subset M of $\mathbb{N}\backslash\{1\}$, we obtain $\left(\frac{w^n}{M}\right)_S = S$ and $\langle w^n\rangle^+ = \{w^n\}$. Hence $\left(\frac{w^n}{M}\right)_S \not\subseteq \langle w^n\rangle^+$.

1. Proofs

In this section, let S always denote a semiring. Let us consider the natural pre-order $\leq_S$ on S defined for $a, b \in S$ in the following manner: $a \leq_S b$ if and only if $a = b$ or $a + c = b$ for some $c \in S$. We also view S naturally as a unitary $\mathcal{D}(S)$-semimodule, where $\mathcal{D}(S)$ is the semiring extending S with a multiplicative unit added freely. For an element $a \in S$, let $\mathrm{ord}(a)$ denote the *order of* a (i.e. $\mathrm{ord}(a)$ is the cardinality of the semigroup $\langle a\rangle^+$).

Results 1.1. We shall use the following results (here $\mathbb{Z}$ denotes the set of all integers):

(i) [7, Theorem 2.3] In a finitely generated commutative semigroup A, an element $a \in A$ is torsion provided that there is $b \in \langle a\rangle^+$ and an infinite set $M \subseteq \mathbb{N}$ such that b is M-divisible in A.

(ii) [5, Lemma 2.3] Let $z \in S$ and $m \in \mathbb{N}$ be such that the set $\left(\frac{z}{m}\right)_{\mathcal{D}(S)z}$ is non-empty. If $u, v \in \mathcal{D}(S)z$ and $mu = mv$, then $u = v$.

(iii) [7, Theorem 1.2] For $w \in S$ and $n, k \in \mathbb{N}$ the set

$$^k\Pi_{w,n}(S) := \{\ell \in \mathbb{Z} \,|\, n + \ell > 0 \ \ \& \ \ k \cdot w^{n+\ell} \leq_S k \cdot w^n\}$$

is of the form $^k\Pi_{w,n}(S) = \{d \cdot n_0, d \cdot (n_0 + 1), \ldots, -d, 0, d, \ldots\}$ for some $n_0 < 0 < d$ provided that $^k\Pi_{w,n}(S)$ contains at least one positive and at least one negative integer.

(iv) [4, Theorem 5.1] Let R be a finitely generated commutative ring. Then there are a finite subset of primes P and a free commutative subgroup F of the additive group $(R, +)$ such that R/F is a P-group.

To prove the Theorems 0.1 and 0.3, we will need a few lemmas. In the beginning, let us recall that for an element $a \in S$ the semigroup $\langle a\rangle^+$ is a group if and only if there is $k \in \mathbb{N}$ such that $a = a + ka$.

Lemma 1.2. *Let $(A, +)$ be a semigroup and let $a, b, c, z \in A$ and $j, k, \ell, m \in \mathbb{N}$.*

(i) *If $a = a + c$, then $a = a + nc$ for every $n \in \mathbb{N}$. If, moreover, $b \geq_A a$, then $b = b + nc$.*

(ii) *If $m \geq j$ and $ja = (j + k)a$, then $ma = (1 + k)ma$.*

(iii) *If* $b \geq_A \big(k \cdot \operatorname{ord}(kz)\big) \cdot z$, *then there is* $\ell \in \mathbb{N}$ *such that* $b = b + \ell kz$. *In particular, if* $m \geq k \cdot \operatorname{ord}(kz)$ *then,* $mz = (1 + \ell k)mz$.

(iv) *If* $a = c + z$ *and* $z = ma$, *then for every* $i \geq 0$ *is* $a = (\sum_{j=0}^{i} m^j)c + m^i z$.

(v) *If* $\gcd(k, m) = 1$, *then there is* $i_0 \in \mathbb{N}$ *such that* $m^{i_0} \equiv 1 \pmod{k}$ *and therefore* $\sum_{j=0}^{i_0 k} m^j \equiv k \sum_{j=0}^{i_0} m^j \equiv 0 \pmod{k}$.

Proof. The items (i) and (iv) follow easily by induction and (v) is well known.

To prove (ii), use (i) for $ma \geq_A ja$ and $ja = ja + ka$.

It remains to show (iii). Since the order of kz is finite, there are $j', \ell \in \mathbb{N}$ such that $j'(kz) = j'(kz) + \ell(kz)$ and $j' \leq \operatorname{ord}(kz)$. Therefore, we have

$$b \geq_A (k \cdot \operatorname{ord}(kz)) \cdot z \geq_A j'kz.$$

Now, it remains to use the item (i) in a suitable way. Finally, the particular case, when we assume $m \geq k \cdot \operatorname{ord}(kz)$, follows from the inequality $mz \geq_A (k \cdot \operatorname{ord}(kz)) \cdot z$ with help of the item (i), again. □

Lemma 1.3. *Let* $(A, +)$ *be a semigroup. Let* $z \in A$ *be a torsion element and* $a \in (\frac{z}{\mathbb{N}\setminus\{1\}})_A$ *be such that* $a \geq_A z$. *Then both* $\langle z\rangle^+$ *and* $\langle a\rangle^+$ *are groups.*

Proof. By our assumption, there is $m \geq 2$ such that $z = ma$. By Lemma 1.2(iv), we have $a \geq_A m^n z$ for every $n \in \mathbb{N}$. Now, there is $n_0 \in \mathbb{N}$ such that $m^{n_0} \geq \operatorname{ord}(z)$, hence $a \geq_A m^{n_0} z \geq_A \operatorname{ord}(z) \cdot z$. By Lemma 1.2(iii), there is $\ell \in \mathbb{N}$ such that $a = a + \ell z = a + \ell ma$. This implies that $\langle a\rangle^+$ and $\langle z\rangle^+$ are groups. □

Lemma 1.4. *Let* $z \in S$ *be torsion. If the set* $(\frac{z}{\mathbb{N}\setminus\{1\}})_{\mathcal{D}(S)z}$ *is non-empty then* $\langle z\rangle^+$ *is a group and* $(\frac{z}{\mathbb{N}})_{\mathcal{D}(S)z} \subseteq \langle z\rangle^+$.

Proof. Let $a \in \mathcal{D}(S)z$ and $m \geq 2$ be such that $z = ma$. Since z is torsion, there is $n_0 \in \mathbb{N}$ such that $m^{n_0} \geq \operatorname{ord}(z)$. By Lemma 1.2(iii), there is $\ell \in \mathbb{N}$ such that $m^{n_0} z = (1 + \ell)m^{n_0} z$. Using Results 1.1(ii) repeatedly, we obtain $z = (1 + \ell)z$. Therefore $\langle z\rangle^+$ is a cyclic group.

Now, let us show that for $N := \operatorname{ord}(z)$, we have $\gcd(m, N) = 1$. Suppose, on the contrary, that $\gcd(m, N) = d > 1$. Set $j := \frac{N}{d}$, $k := \frac{m}{d}$ and $u := ka$. Since $u \in \mathcal{D}(S)z$, we can multiply the equality $z = (1 + N)z$ by a suitable element from $\mathcal{D}(S)$ and obtain $u = (1 + N)u$. From $z = ma = dka = du$ it follows that $u = u + jdu = u + jz$. As $z \geq_S u$, we obtain $z = (1 + j)z$, by Lemma 1.2(i). This is a contradiction with the order N of the group $G := \langle z\rangle^+$.

Finally, since G is a cyclic group of order N and $\gcd(m, N) = 1$, there is $b \in G \subseteq \mathcal{D}(S)z$ such that $z = mb$. According the uniqueness in Results 1.1(ii), we obtain $a = b \in G = \langle z\rangle^+$. Therefore $\left(\frac{z}{\mathbb{N}}\right)_{\mathcal{D}(S)z} \subseteq \langle z\rangle^+$. □

Lemma 1.5. *Let* $z \in S$. *If* $k, m \in \mathbb{N}$ *are such that the set* $(\frac{kz}{m})_{\mathcal{D}(S)z}$ *is non-empty and* $\frac{m}{k} \geq \operatorname{ord}(kz)$, *then* $\langle kz\rangle^+$ *is a group.*

Proof. There is an element $a \in \mathcal{D}(S)z$ such that $kz = ma$. Since $m \geq k \cdot \operatorname{ord}(kz)$, by Lemma 1.2(iii), there is $\ell \in \mathbb{N}$ such that $mz = (1 + \ell k)mz$. By multiplying this equality by a suitable element from $\mathcal{D}(S)z$, we obtain $ma = (1 + \ell k)ma$ as well. As $kz = ma$, it is therefore seen that $\langle kz \rangle^+$ is a group. □

Lemma 1.6. *Let $w \in S$, $k, n \in \mathbb{N}$ and let ${}^k\Pi_{w,n}(S)$ contain some negative integer. If $a \in (\frac{kw^n}{\mathbb{N}})S$ and if $i \in \mathbb{N}$, $i \geq n$ are such that $a \geq_S kw^i$, then $a \geq_S kw^n$.*

Proof. The set $K := \{i' \in \mathbb{N} \,|\, i' \geq n \,\&\, a \geq_S kw^{i'}\}$ is non-empty. Put $i_0 := \min(K)$.

Assume on the contrary, that $i_0 > n$. Since $kw^n = ma \geq_S a \geq_S kw^{i_0}$, the set ${}^k\Pi_{w,n}(S)$ contains a positive integer $i_0 - n$. Therefore, by Results 1.1(iii), for the least positive element d of ${}^k\Pi_{w,n}(S)$ it holds that $-d \in {}^k\Pi_{w,n}(S)$. By the choice of d, we obtain $i_0 - n \geq d$. Since $-d \in {}^k\Pi_{w,n}(S)$, it follows that $kw^n \geq_S kw^{n-d}$. Multiplying this inequality by w^{i_0-n}, we obtain

$$a \geq_S kw^{i_0} = w^{i_0-n} \cdot kw^n \geq_S w^{i_0-n} \cdot kw^{n-d} = kw^{i_0-d}.$$

Moreover, $n \leq i_0 - d$ and therefore the element $i_0 - d$ belongs to K. This is a contradiction with the choice of i_0.

We have shown that $\min(K) = n$. Thus $a \geq_S kw^n$. □

Now, let us prove the theorems of this paper. We start with the proof of Theorem 0.2.

Proof of Theorem 0.2. The implication (i) ⇒ (ii) is easy. To prove the implication (ii) ⇒ (i), let us first assume that A is finite. Since M is infinite, there are $m_1, m_2 \in M$, $m_1 < m_2$ and $a \in A$ such that $m_1 a = z = m_2 a$. By Lemma 1.2(ii), we have $m_1 a = (1 + \ell)m_1 a$, where $\ell = m_2 - m_1 > 0$. Since $z = m_1 a$, we see that $\langle z \rangle^+$ a group.

Let us prove the general case. Since A is residually finite, we can assume that A is a subsemigroup of $\prod_{i \in I} A_i$, where I is a set and for every $i \in I$, A_i are finite commutative semigroups. Let $z = \{z_i\}_{i \in I} \in A$, where $z_i \in A_i$ for every $i \in I$, be M-divisible for an infinite set $M \subseteq \mathbb{N}$. Consequently, for every $i \in I$ the element z_i is also M-divisible in A_i and, by the first part of the proof, z_i generates a group. By Results 1.1(i), the element z is torsion. Hence, there are $n, k \in \mathbb{N}$ such that $nz = (n + k)z$. It follows that $nz_i = (n + k)z_i$ for every $i \in I$. Since z_i generates a group, we obtain $z_i = (k + 1)z_i$. Finally, $z = \{z_i\}_{i \in I} = \{(k + 1)z_i\}_{i \in I} = (k + 1)z$. As a result, z generates a group. □

Proof of Theorem 0.1. The implication (i) ⇒ (ii) is obvious. To prove the implication (ii) ⇒ (i), choose $k, n \in \mathbb{N}$ and assume that there is an infinite set of primes P, and for every $p \in P$ there is $a_p \in S$ such that $kw^n = p \cdot a_p$. By Theorem A, the element kw^n is torsion. Set

$$P_1 := \{p \in P \,|\, p \geq k \cdot \operatorname{ord}(kw^n) \;\;\&\;\; (\exists i \in \mathbb{N})\ i < n \;\&\; a_p \geq_S w^i\}$$

and

$$P_2 := \{p \in P \,|\, p \geq k \cdot \operatorname{ord}(kw^n) \ \ \& \ \ (\exists i \in \mathbb{N})\ i \geq n \ \&\ a_p \geq_S w^i\}.$$

Let us now distinguish the following three cases:

(i) Let $P_2 = \emptyset$. Then the set P_1 is infinite and kw^n is a P_1-divisible element in the semigroup $\langle w, w^2, \dots, w^n\rangle^+$. Hence, by Proposition 0.2, $\langle kw^n\rangle^+$ is a group.

(ii) Let $P_1 = \emptyset$. Then the set P_2 has to be non-empty. Let us choose a prime $p \in P_2$. Since $p \notin P_1$, we see that $a_p \in \mathcal{D}(S)w^n$. Thus $a_p \in (\frac{kw^n}{p})_{\mathcal{D}(S)w^n}$ and, by Lemma 1.5, we obtain that $\langle kw^n\rangle^+$ is a group.

(iii) Finally, assume that both the sets P_1 and P_2 are non-empty. Choose $p \in P_1$ and $q \in P_2$.

First, let us show that there is an element $a \in (\frac{kw^n}{q})_S$ such that $a \geq_S kw^n$. Since $p \in P_1$, there is $i_0 \in \mathbb{N}$ such that $i_0 < n$ and $a_p \geq_S w^{i_0}$. Therefore $kw^n = pa_p \geq_S ka_p \geq_S kw^{i_0}$ and ${}^k\Pi_{w,n}(S)$ contains a negative integer $i_0 - n$.

We already know that the element kw^n is torsion and from $q \geq k \cdot \operatorname{ord}(kw^n)$, by Lemma 1.2(iii), we have $qw^n = (1 + \ell k)qw^n$ for some $\ell \in \mathbb{N}$.

Further, since $q \in P_2$, there is $i \in \mathbb{N}$ such that $i \geq n$ and $a_q \geq_S w^i$. Therefore, multiplying the previous equality by w^{i-n}, we obtain $qw^i = qw^i + q\ell kw^i$. Since $qa_q \geq_S qw^i$, it follows, by Lemma 1.2(i), that $qa_q = qa_q + q\ell kw^i$. Now, simply set $a := a_q + \ell kw^i$. Finally, we can apply Lemma 1.6 and obtain that $a \geq_S kw^n$.

We have found the desired element a. Now, by Lemma 1.3, $\langle kw^n\rangle^+$ is a group.

Now we prove the second equivalence. The implication (iii) ⇒ (iv) is obvious. To prove the implication (iv) ⇒ (iii), let us assume that $z := kw^n$ is divisible in S. By the first part of the proof, $\langle z\rangle^+$ is a group. We are going to prove that z has to be idempotent.

First, let us show that z is divisible within the semigroup $\langle w, w^2, \dots, w^n\rangle^+$. Since z generates a group, there is a neutral element $o := Nz$ in the group $\langle z\rangle^+$, where $N := \operatorname{ord}(z)$. As z is divisible in S, for every $\ell \in \mathbb{N}$ there are $b \in \langle w, w^2, \dots, w^n\rangle^+$ and $\alpha \in \mathcal{D}(S)$ such that $z = \ell kN(b + \alpha w^n)$.

We show that we can, in fact, always choose α to be equal to 1. Since αo is idempotent, we have

$$z = \ell kNb + \ell\alpha(Nkw^n) = (\ell kN)b + \ell\alpha o = (\ell kN)b + \alpha o.$$

Further,

$$2z = 2(\ell kN)b + 2\alpha o = (\ell kN)b + ((\ell kN)b + \alpha o) = (\ell kN)b + z$$

and, using the inverse of the element z, we obtain

$$z = (\ell kN)b + o = (\ell kN)b + (\ell kN)w^n = (\ell kN)(b + w^n).$$

Hence, z is a divisible element in the semigroup $\langle w, w^2, \dots, w^n\rangle^+$. Thus, by Theorem B, the element z is idempotent. □

For the sake of simplicity, put $C_k := \{m \in \mathbb{N} \mid \gcd(m,k) = 1\}$ for $k \in \mathbb{N}$.

Proof of Theorem 0.3. First, consider that w^n is not torsion. Then, by Theorem A, there are only finitely many primes $p_1, \dots, p_j$ that do not divide w^n. We can set $k := p_1 \cdots p_j$ and immediately obtain that $(\frac{w^n}{C_k})_S = \{w^n\}$.

Now, assume that w^n is torsion. In this case, set $k := \operatorname{ord}(w^n)$. Let $a \in S$ and $m \in \mathbb{N}$ be such that $\gcd(m,k) = 1$ and $w^n = ma$. There are $f, g \in x \cdot \mathbb{N}[x]$ such that $a = f(w)w^{n-1} + g(w)$ and $\deg(g) \le n-1$. Let us divide the rest of the proof into three cases (i)–(iii). We will need the assumption that $\gcd(m,k) = 1$ only in the third case.

(i) If $g = 0$ then, by Lemma 1.4, $a \in \langle w^n \rangle^+$.
(ii) If $f = 0$, then $a \in \langle w, w^2, \dots, w^{n-1} \rangle^+$.
(iii) Let $g \neq 0$ and $f \neq 0$. Then, by Lemma 1.6, $a \ge_S z := w^n$.

Therefore, by Lemma 1.3, both $\langle z \rangle^+$ and $\langle a \rangle^+$ are groups with a common additively neutral element o. Further, from $a \ge_S z = w^n$ it follows that there are $b \in \langle w, w^2, \dots, w^n \rangle^+$ and $\alpha \in \mathcal{D}(S)$ such that $a = \alpha z + b + z$.

We are going to eliminate the component αz. Since $z = (1+k)z$, we obtain $\alpha z = \alpha z + k\alpha z$. By Lemma 1.2(i), the inequality $a = \alpha z + b + z \ge_S \alpha z$ implies the equality $a = a + k\alpha z$. This yields $o = o + k\alpha z$.

Now, we use the assumption $\gcd(m,k) = 1$. By Lemma 1.2(v), there is $i_0 \in \mathbb{N}$ such that $\sum_{j=0}^{i_0 k} m^j = \ell \cdot k$ for some $\ell \in \mathbb{N}$. Applying Lemma 1.2(iv) on $a = (\alpha z + b) + z$ and $z = ma$, we obtain that

$$a = o + a = o + (\ell \cdot k(\alpha z + b) + m^{i_0 k} z) = (o + \ell \cdot k\alpha z) + \ell k b + m^{i_0 k} z$$

$$= o + \ell k b + m^{i_0 k} z = \ell k b + m^{i_0 k} z \in \langle w, w^2, \dots, w^n \rangle^+.$$

Summing this up, we have $a \in \langle w, w^2, \dots, w^n \rangle^+$. Hence $(\frac{w^n}{C_k})_S \subseteq \langle w, w^2, \dots, w^n \rangle^+$. □

Proof of Theorem 0.4. Let us divide the proof into the torsion and torsion-free cases.

(i) First, assume that G is torsion. Let T be the torsion part of $(R,+)$. Since R is noetherian, the ideal T of R is finitely generated and there is $k \in \mathbb{N}$ such that $kT = 0$.

Now, let $a \in (\frac{G}{C_k})_R$ and $m \in C_k$ be such that $ma \in G \subseteq T$. Then a is a torsion element. It follows that $ka = 0 \in G$. Since $\gcd(m,k) = 1$, we obtain that $a \in G$. Therefore $(\frac{G}{C_k})_R \subseteq G$.

(ii) Further, suppose that R is torsion-free. By Results 1.1(iv), there is a free commutative group $F \subseteq R$ and a finite set of primes $P_0 = \{p_1, \dots, p_\ell\}$ such that R/F is a P_0-group. Since G is a finitely generated group, there is $i \in \mathbb{N}$ such that for $n_0 := (p_1 \cdots p_\ell)^i$, we have $G_1 := n_0 G \subseteq F$.

The group G_1 is also finitely generated and therefore there are free commutative groups $F_1, F_2 \subseteq F$ such that $G_1 \subseteq F_1$, the group F_1 is finitely generated, the group F_1/G_1 is finite and $F = F_1 \oplus F_2$. Thus, there is $n_1 \in \mathbb{N}$ such that $n_1 F_1 \subseteq G_1 = n_0 G$.

Now, set $k := n_1 \cdot p_1 \cdots p_\ell$. Let $a \in (\frac{G}{C_k})_R$ and $m \in C_k$ be such that $ma \in G$. Set $b := n_0 a \in R$. Then $mb = m(n_0 a) \in n_0 G = G_1 \subseteq F_1$.

Further, since R/F is a P_0-group, there is a suitable $j \in \mathbb{N}$ such that for $m_0 := (p_1 \cdots p_\ell)^j$, we have $c := m_0 b \in F$ and $mc = m_0(mb) \in F_1$. As F_1 is a direct summand of F, we obtain that $m_0 b = c \in F_1$, as well.

Finally, from $m_0 b, mb \in F_1$ and $\gcd(m_0, m) = 1$ it follows that $b \in F_1$. Therefore $n_0(n_1 a) = n_1 b \in n_1 F_1 \subseteq G_1 = n_0 G$. Since the group $(R, +)$ is torsion-free, we can infer that $n_1 a \in G$. Combining $ma, n_1 a \in G$ and $\gcd(m, n_1) = 1$, we obtain that $a \in G$. Therefore $(\frac{G}{C_k})_R \subseteq G$.

(iii) To end the reasoning up, we prove the general case. Let T be the ideal of all torsion elements of R. Set $H := G \cap T$. By (i), there is $k_1 \in \mathbb{N}$ such that $(\frac{H}{C_{k_1}})_R \subseteq H$. Similarly, by (ii), there is $k_2 \in \mathbb{N}$ such that $(\frac{(G+T)/T}{C_{k_2}})_{R/T} \subseteq (G + T)/T$. Now, put $k := k_1 \cdot k_2$ and the rest follows easily by a standard argument. □

References

[1] J. Araújo and M. Kinyon, Inverse semigroups with idempotent-fixing automorphisms, *Semigroup Forum* **89**(2) (2014) 469–474.

[2] W. E. Clark, W. C. Holland and G. J. Székely, Decompositions in discrete semigroups, *Studia Sci. Math. Hungar.* **34** (1998) 15–23.

[3] P. A. Grillet, *Semigroups: An Introduction to the Structure Theory* (Marcel Dekker, Inc., New York, 1995).

[4] M. Kechlibar, T. Kepka and J. Kortelainen, A note on finitely generated commutative rings, *Acta Univ. Carolin. Math. Phys.* **46**(1) (2005) 101–105.

[5] T. Kepka and M. Korbelář, Conjectures on additively divisible commutative semirings, *Math. Slovaca* **66**(5) (2016) 1059–1064.

[6] V. N. Kolokoltsov and V. P. Maslov, *Idempotent analysis and its applications*, Mathematics and Its Applications, Vol. 401 (Springer, Netherlands, 1997).

[7] M. Korbelář, Torsion and divisibility in finitely generated commutative semirings, *Semigroup Forum* (2016) 10p, doi: 10.1007/s00233-016-9827-4.

[8] M. Korbelář and G. Landsmann, One-generated semirings and additive divisibility, *J. Algebra Appl.* **16**(2) (2017) 22p, doi: 10.1142/S0219498817500384.

[9] D. Maclagan and B. Sturmfels, *Introduction to Tropical Geometry*, Graduate Studies in Mathematics, Vol. 161 (American Mathematical Society, Providence, Rhode Island, 2015).

[10] A. I. Mal'cev, On homomorphisms into finite groups, *Lecture Notes of Ivanovsk Pedagog. Inst.* **18** (1958) 49–60 [translated in: *Twelve Papers in Algebra*, ed. L. J. Leifman (American Mathematical Society, 1983), pp. 67–79].

Research Article

Vítězslav Kala and Miroslav Korbelář*

Idempotence of finitely generated commutative semifields

https://doi.org/10.1515/forum-2017-0098
Received May 3, 2017; revised January 30, 2018

Abstract: We prove that a commutative parasemifield S is additively idempotent, provided that it is finitely generated as a semiring. Consequently, every proper commutative semifield T that is finitely generated as a semiring is either additively constant or additively idempotent. As part of the proof, we use the classification of finitely generated lattice-ordered groups to prove that a certain monoid associated to the parasemifield S has a distinguished geometrical property called prismality.

Keywords: Commutative semiring, parasemifield, idempotent, convex, affine monoid

MSC 2010: Primary 12K10, 16Y60, 20M14; secondary 11H06, 52A20

Communicated by: Manfred Droste

1 Introduction

It is easy to see that the field $\mathbb{Q}$ of rational numbers is not finitely generated as a ring. More generally, a *folklore* theorem (perhaps due to Kaplansky) states that if a commutative ring is simple and finitely generated, then it is finite. Of course, such rings are precisely the finite fields $\mathbb{F}_q$ and the zero-multiplication rings $\mathbb{Z}_p$ of prime order. This result can also be viewed as a classification of all finitely generated simple commutative rings.

Semirings often behave similar to rings (see, e.g., [14] for an overview). Thus, it is natural to ask whether a similar result as above also holds in the more general setting of semirings. In this paper we will not consider the other natural generalization to non-commutative rings; in fact, all algebraic structures will be commutative throughout the paper. Nevertheless, let us mention at least one of the latest results on simple non-commutative rings [6].

Definition 1.1. Recall that by a (commutative) *semiring* we mean a non-empty set S equipped with two associative and commutative operations (addition and multiplication), where the multiplication distributes over the addition from both sides. A semiring S is a *semifield* if it contains a zero element 0 and the set $S \setminus \{0\}$ is a group with respect to the multiplication. In the case that the entire multiplicative part $S(\cdot)$ is a group, the semiring S is called a *parasemifield*. A semiring (a semifield, resp.) is called *proper* if it is not a ring. Finally, a semiring S is *additively idempotent* if $x + x = x$ for all $x \in S$ and *additively constant* if the map $S \times S \to S$, $(x, y) \mapsto x + y$, is constant.

Vítězslav Kala, Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic; and University of Göttingen, Mathematisches Institut, Bunsenstr. 3-5, D-37073 Göttingen, Germany, e-mail: vita.kala@gmail.com. http://orcid.org/0000-0001-5515-6801
***Corresponding author: Miroslav Korbelář,** Department of Mathematics, Faculty of Electrical Engineering, Czech Technical University in Prague, Technická 2, 166 27 Prague 6, Czech Republic, e-mail: miroslav.korbelar@gmail.com. http://orcid.org/0000-0002-9751-3261

In mathematics, semirings and semifields are ubiquitous, which makes them one of the fundamental algebraic objects. The first mathematical structure one encounters, the set of natural numbers $\mathbb{N}$, is a semiring. Besides this obvious observation, semirings and semifields play an important role in modern mathematics as well as in a wide range of applications. Let us mention a few of them. Tropical geometry, which is essentially algebraic geometry over additively idempotent semirings, is useful in studying piecewise linear functions in optimization problems (see, e.g., [13, 16, 17] and the references therein). Tropical semirings are also used in constructing cluster algebras [24] and appear in the process of so-called dequantization [27]. In number theory, Connes and Consani [7, 8] were motivated by the goal of working over the "field of one element" [34] (related to semirings) and extended this viewpoint further with a certain hope of proving Riemann hypothesis. Their work was recently generalized by Leichtnam [26] to cover more general additively idempotent semifields. An interesting direction is also the study of cryptography based on semirings, as developed by Maze, Monico, Rosenthal, Zumbrägel, and others [28, 29, 38]. It could help in coping with some of the vulnerabilities of classical cryptography based on modular arithmetic. Semirings are also important for weighted automata in theoretical computer science [11]. Yet another class of applications arises thanks to the correspondence between certain semifields, lattice-ordered groups, and MV-algebras. These provide useful tools in multi-valued logic [1–3, 9, 10, 30, 31]. For further applications and references, see, e.g. [14, 15, 23].

In this paper we are interested in studying finitely generated simple semirings. Unfortunately, the situation quickly becomes more convoluted than in the case of rings. First of all, ideals in semirings do not correspond to congruences, and so one has to distinguish between *congruence-* and *ideal-simple* semirings (i.e., those that have only the trivial congruences, and those in which there are no proper ideals). Both of these cases were (almost completely) classified by Bashir, Hurt, Jančařík and Kepka [12]. It has turned out that there are semirings which are finitely generated, both congruence- and ideal-simple, and yet *infinite* – for instance, the additively idempotent tropical semiring $\mathbb{Z}(\oplus, \odot)$ with the semiring addition $a \oplus b = \min(a, b)$ and multiplication $a \odot b = a + b$. On the other hand, every *finite* congruence- or ideal-simple *proper* semiring is either additively constant or additively idempotent [12].

Hence, we need to modify the *folklore* theorem to also deal with these cases. For congruence-simple semirings, this quite easily follows from the classification using [12, Corollary 14.3]: Every proper finitely generated congruence-simple semiring is either additively constant or additively idempotent.

The main result of this paper is the proof of an analogous result for ideal-simple semirings.

Theorem 1.2. (a) *Every parasemifield that is finitely generated as a semiring is additively idempotent.*
(b) *Every proper semifield that is finitely generated as a semiring is either additively constant or additively idempotent.*
(c) *Every proper finitely generated ideal-simple semiring is either additively constant or additively idempotent.*

This statement can be now understood as an extension of the *folklore* theorem referred in the beginning, i.e., that every (commutative) field that is finitely generated as a ring is finite. Of course, the greatest difference is the existence of additively idempotent semifields.

Since every semifield is clearly ideal-simple, part (b) of the theorem follows immediately from (c). Also, one can be slightly more precise in the additively constant case. This occurs if and only if there is a finitely generated (multiplicative) abelian group $G(\cdot)$ and the semiring is the semifield $S := G \cup \{o\}$, where o is a new element. Operations that extend the multiplication on G are defined by $a + b = o$ and $a \cdot o = o$ for all $a, b \in S$.

Theorem 1.2 was at first formulated as a conjecture in [12] for the infinite cases. Our version is a slight modification that considers *proper* semirings instead of *infinite* ones and that includes in this way also the finite cases, whose properties were mentioned above. The equivalence of (a) and (c) was then established by Ježek, Kala and Kepka [19, 21], and so it remained to prove (a). Initial steps in this direction were done by the present authors and Kepka [22], and continued together with Ježek [18], where part (a) was proved in the case of 2 generators. Note that there are no parasemifields that are 1-generated as semirings [22, Remark 4.22].

As we already mentioned, the goal of this paper is to prove Theorem 1.2 in general (by proving Theorem 4.5) and to settle in this way a problem that remained open for more than fifteen years. The general idea of the proof uses a suitable subsemiring Q_S of the parasemifield S and an associated monoid $\mathcal{C}_X(S) \subseteq \mathbb{N}_0^n$ (see Section 3 for the definitions). In the 2-generated case [18], the monoid $\mathcal{C}_X(S)$ was simple enough to consider only elementary properties of the geometry to prove the theorem. However, in the general case the monoid has a much more complicated shape, and so the situation is significantly harder.

One key ingredient in our proof comes from the classification of finitely generated lattice-ordered groups (ℓ-groups) by Busaniche, Cabrer and Mundici [5]. There is a well-known term-equivalence between ℓ-groups and additively idempotent parasemifields, and so Kala [20] has recently used their results to obtain a classification of additively idempotent parasemifields which are finitely generated as semirings (see Definition 3.3 below). The monoid $\mathcal{C}_X(T)$ associated to each of these additively idempotent parasemifields T has a special geometric property, *prismality* (introduced in Section 2). Now given a general parasemifield S that is finitely generated as a semiring, we consider its largest factor-parasemifield that is additively idempotent. The associated monoids of both these parasemifields are the same, and so we conclude that the monoid of S is also prismal. This then gives us the crucial missing geometrical information that allows us to finish the proof of Theorem 4.5 (and thus also of Theorem 1.2).

As in the case of rings, these results then imply a classification of all finitely generated ideal-simple semirings. If such a semiring is, moreover, a parasemifield then it must be one from Definition 3.3. The extension to general ideal-simple semirings is then a routine application of the classification theorems of [12, 19], and so we do not state it explicitly here. Note that an analogous result was recently proved by Schneider and Zumbrägel for simple compact (not necessarily commutative) semirings [33].

As for the organization of the paper, in the second section we introduce a property of submonoids of $(\mathbb{Z}^n, +)$ called *prismality* and study its basic properties. In the third section we prove in Theorem 3.8 that every monoid $\mathcal{C}_X(S)$ associated to a finite set X, that generates a parasemifield S as a semiring, is prismal. Finally, the fourth section uses this result to prove Theorem 4.5.

Let us conclude this introduction by pointing out that the ideas presented in this paper can probably be generalized to the situation of additively divisible semirings. Another very interesting generalization of our results and methods is to apply them to the Banach semifield setting of Leichtnam [26]. This should (hopefully) allow us to generalize and extend his results (e.g., to remove Assumption 2) – we also plan to study this in the (near) future.

2 Prismal monoids

In this section we define a property of submonoids of $(\mathbb{Z}^n, +)$ called *prismality* and study its behavior.

First, we need some definitions. Every vector space considered in this paper is assumed to be a *real* vector space. A vector subspace $V \subseteq \mathbb{R}^n$ is said *to be defined over* $\mathbb{Q}$ if V has a basis that consists of vectors from $\mathbb{Q}^n$. Of course, this is equivalent to assuming that V has a basis of vectors from $\mathbb{Z}^n$.

Let M be a subset of $\mathbb{R}^n$. By $\langle M\rangle$ we denote the *vector subspace of* $\mathbb{R}^n$ *generated by* M, by $\overline{M}^{\mathbb{R}^n}$ the usual *topological closure of* M and by $\operatorname{conv}(M)$ the *convex hull of* M. Further, we denote by $\dim(M)$ the *dimension of the convex hull* $\operatorname{conv}(M)$. Note that in the case when M is a cone or a monoid, this is the dimension of the vector space $\langle M\rangle$.

By a *cone* $K \subseteq \mathbb{R}^n$ we mean a convex set such that for every non-negative real number λ and every $u \in K$, we have $\lambda u \in K$. When working with a convex set $A \subseteq \mathbb{R}^n$, we will use the notion of the *relative interior of* A, denoted as $\operatorname{ri}(A)$, that is defined as the interior of A with respect to the affine hull of A.

Definition 2.1. For a submonoid $\mathcal{C}$ of $(\mathbb{Z}^n, +)$ define its *closure* $\overline{\mathcal{C}}$ as

$$\overline{\mathcal{C}} = \mathbb{Z}^n \cap \overline{\operatorname{conv}(\mathcal{C})}^{\mathbb{R}^n}.$$

Further put

$$\sqrt{\mathcal{C}} = \{\alpha \in \mathbb{Z}^n \mid \text{there exists } k \in \mathbb{N} \text{ such that } k\alpha \in \mathcal{C}\}.$$

We say that a monoid $\mathcal{C} \subseteq \mathbb{Z}^n$ is

- *pure* if $\sqrt{\mathcal{C}} = \mathcal{C}$,
- *almost prismal* if for every vector subspace V of $\mathbb{R}^n$, the monoid $\overline{\mathcal{C} \cap V}$ is finitely generated,
- *prismal* if it is pure and almost prismal.

Finitely generated monoids are often called *affine* (although we will not use this terminology). As is clear from the definition, almost prismal monoids are a generalization of affine monoids.

We will be interested in properties of prismal monoids, namely, whether they are closed under intersections, products and homomorphic images. The answer is "Yes!", but the arguments are not entirely easy, and one has to be a little careful, as for example Remark 2.6 shows.

Before we can prove the closedness in Theorems 2.5, 2.10 and 2.11, we will need some technical results on cones and monoids. These are essentially known, but not easily located in the literature, so we also include (most of) their proofs.

Proposition 2.2 ([32, Theorems 6.3 and 6.5]). *Let $K, L \subseteq \mathbb{R}^n$ be cones. Then*
(i) $\mathrm{ri}(\overline{K}^{\mathbb{R}^n}) = \mathrm{ri}(K)$ *and* $\overline{K}^{\mathbb{R}^n} = \overline{\mathrm{ri}(K)}^{\mathbb{R}^n}$,
(ii) $\mathrm{ri}(K \cap L) = \mathrm{ri}(K) \cap \mathrm{ri}(L)$ *if* $\langle K\rangle = \langle L\rangle = \langle K \cap L\rangle$.

Proposition 2.3. *Let $\mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}^n$ be pure monoids. Then*
(i) $\mathbb{Z}^n \cap \mathrm{conv}(\mathcal{C}) = \mathcal{C}$,
(ii) $\mathrm{conv}(\mathcal{C}) \cap \mathrm{conv}(\mathcal{D}) = \mathrm{conv}(\mathcal{C} \cap \mathrm{conv}(\mathcal{D})) = \mathrm{conv}(\mathcal{C} \cap \mathcal{D})$.

Proof. (i) Every $\alpha \in \mathbb{Z}^n \cap \mathrm{conv}(\mathcal{C})$ is a convex linear combination of a finite affinely independent subset of $\mathcal{C}$. Hence, the coefficients in this combination have to be rational and, due to the convexity, also non-negative. Thus, there is $k \in \mathbb{N}$ such that $k\alpha \in \mathcal{C}$. Since $\mathcal{C}$ is pure, we obtain that $\alpha \in \mathcal{C}$. The other inclusion is obvious.

(ii) By (i), we see that $\mathcal{C} \cap \mathrm{conv}(\mathcal{D}) = \mathcal{C} \cap (\mathrm{conv}(\mathcal{D}) \cap \mathbb{Z}^n) = \mathcal{C} \cap \mathcal{D}$. Hence, it is enough to show that $\mathrm{conv}(\mathcal{C}) \cap \mathrm{conv}(\mathcal{D}) = \mathrm{conv}(\mathcal{C} \cap \mathcal{D})$. This assertion holds if $\mathcal{C}$ and $\mathcal{D}$ are finitely generated (see [4]). For the general case, let $y \in \mathrm{conv}(\mathcal{C}) \cap \mathrm{conv}(\mathcal{D})$. Then $y \in \mathrm{conv}(\mathcal{C}') \cap \mathrm{conv}(\mathcal{D}')$ for some finitely generated submonoids $\mathcal{C}' \subseteq \mathcal{C}$ and $\mathcal{D}' \subseteq \mathcal{D}$. Hence, we have $y \in \mathrm{conv}(\mathcal{C}' \cap \mathcal{D}') \subseteq \mathrm{conv}(\mathcal{C} \cap \mathcal{D})$. The other inclusion is obvious. □

Proposition 2.4. *Let $\mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}^n$ be pure monoids and V a vector subspace of $\mathbb{R}^n$. Then*

$$\overline{(\mathcal{C} \cap \mathcal{D}) \cap V} = \overline{\mathcal{C} \cap W} \cap \overline{\mathcal{D} \cap W},$$

where $W = \langle \mathcal{C} \cap \mathcal{D} \cap V\rangle$.

Proof. Set $\mathcal{C}' = \mathcal{C} \cap W$ and $\mathcal{D}' = \mathcal{D} \cap W$. Then $(\mathcal{C} \cap \mathcal{D}) \cap V = \mathcal{C}' \cap \mathcal{D}'$. Hence, $\langle \mathcal{C}' \cap \mathcal{D}'\rangle = W$, and therefore we also have $\langle \mathcal{C}'\rangle = W = \langle \mathcal{D}'\rangle$. Put $M = \overline{\mathrm{conv}(\mathcal{C}')}^{\mathbb{R}^n}$ and $N = \overline{\mathrm{conv}(\mathcal{D}')}^{\mathbb{R}^n}$. Then also $\langle M\rangle = \langle N\rangle = \langle M \cap N\rangle = W$.

By Proposition 2.2 and Proposition 2.3 (ii), we now obtain

$$\begin{aligned}\mathrm{ri}(M \cap N) &= \mathrm{ri}(M) \cap \mathrm{ri}(N) = \mathrm{ri}\big(\overline{\mathrm{conv}(\mathcal{C}')}^{\mathbb{R}^n}\big) \cap \mathrm{ri}\big(\overline{\mathrm{conv}(\mathcal{D}')}^{\mathbb{R}^n}\big)\\ &= \mathrm{ri}(\mathrm{conv}(\mathcal{C}')) \cap \mathrm{ri}(\mathrm{conv}(\mathcal{D}')) = \mathrm{ri}\big(\mathrm{conv}(\mathcal{C}') \cap \mathrm{conv}(\mathcal{D}')\big)\\ &= \mathrm{ri}(\mathrm{conv}(\mathcal{C}' \cap \mathcal{D}')).\end{aligned}$$

Therefore,

$$\overline{\mathrm{conv}(\mathcal{C}')}^{\mathbb{R}^n} \cap \overline{\mathrm{conv}(\mathcal{D}')}^{\mathbb{R}^n} = M \cap N = \overline{M \cap N}^{\mathbb{R}^n} = \overline{\mathrm{ri}(M \cap N)}^{\mathbb{R}^n} = \overline{\mathrm{ri}(\mathrm{conv}(\mathcal{C}' \cap \mathcal{D}'))}^{\mathbb{R}^n} = \overline{\mathrm{conv}(\mathcal{C}' \cap \mathcal{D}')}^{\mathbb{R}^n}.$$

Finally, we obtain the equality

$$\overline{\mathcal{C} \cap W} \cap \overline{\mathcal{D} \cap W} = \mathbb{Z}^n \cap \overline{\mathrm{conv}(\mathcal{C} \cap W)}^{\mathbb{R}^n} \cap \overline{\mathrm{conv}(\mathcal{D} \cap W)}^{\mathbb{R}^n} = \mathbb{Z}^n \cap \overline{\mathrm{conv}(\mathcal{C} \cap \mathcal{D} \cap V)}^{\mathbb{R}^n} = \overline{(\mathcal{C} \cap \mathcal{D}) \cap V}. \qquad \square$$

Theorem 2.5. *Almost prismal monoids are closed under intersections.*

Proof. Let V be a vector subspace of $\mathbb{R}^n$ and let $\mathcal{C}, \mathcal{D}$ be almost prismal monoids. By Proposition 2.4, $\overline{(\mathcal{C} \cap \mathcal{D}) \cap W} = \overline{\mathcal{C} \cap W} \cap \overline{\mathcal{D} \cap W}$ is a finitely generated monoid, as $\overline{\mathcal{C} \cap W}$ and $\overline{\mathcal{D} \cap W}$ are finitely generated. The rest is clear. □

Remark 2.6. Note that in general it need not be true that $\overline{\mathcal{C} \cap \mathcal{D}} = \overline{\mathcal{C}} \cap \overline{\mathcal{D}}$ (which is similar to the case of a usual topological closure operator). An example is when $m = 2$, $\mathcal{C} = \{(i, j) \in \mathbb{N}_0^2 \mid i < j \text{ or } i = j = 0\}$ and $\mathcal{D} = \{(i, j) \in \mathbb{N}_0^2 \mid i > j \text{ or } i = j = 0\}$. Then $\overline{\mathcal{C} \cap \mathcal{D}} = \{(0, 0)\}$, while $\overline{\mathcal{C}} \cap \overline{\mathcal{D}} = \{(k, k) \mid k \in \mathbb{N}_0\}$. Note that in this case, $W = \langle \mathcal{C} \cap \mathcal{D}\rangle = \{(0, 0)\}$ is 0-dimensional.

Proposition 2.7. *Let $\mathcal{C} \subseteq \mathbb{Z}^n$ be a monoid. Then*
(i) *$\mathcal{C}$ is finitely generated if and only if $\sqrt{\mathcal{C}}$ is finitely generated,*
(ii) *$\mathcal{C}$ is almost prismal if and only if for every vector subspace $V \subseteq \mathbb{R}^n$ defined over $\mathbb{Q}$, the monoid $\overline{\mathcal{C} \cap V}$ is finitely generated.*

Proof. It follows easily from the fact that a monoid $\mathcal{C}'$ is finitely generated if and only if the cone $\operatorname{conv}(\mathcal{C}')$ is finitely generated (as a cone), see [4]. □

Lemma 2.8. *Let $V \subseteq \mathbb{R}^n$ be a vector subspace defined over $\mathbb{Q}$ and let $\nu\colon V \to \mathbb{R}^n$ be a linear embedding such that $\nu(V \cap \mathbb{Z}^n) \subseteq \mathbb{Z}^n$. Then $\sqrt{\nu(V \cap \mathbb{Z}^n)} = \nu(V) \cap \mathbb{Z}^n$.*

Proof. Since V is defined over $\mathbb{Q}$, there is a basis $\{u_1, \dots, u_k\} \subseteq \mathbb{Z}^n$ of V. Then $\{\nu(u_1), \dots, \nu(u_k)\} \subseteq \mathbb{Z}^n$ is a basis of $\nu(V)$. For $\alpha \in \nu(V) \cap \mathbb{Z}^n$, there are integers $r_i \in \mathbb{Z}$, $i = 1, \dots, k$, and $s \in \mathbb{N}$ such that $\alpha = \sum_{i=1}^k \frac{r_i}{s}\, \nu(u_i)$. Hence, $s\alpha = \nu(\sum_{i=1}^k r_i\, u_i) \in \nu(V \cap \mathbb{Z}^n)$ and $\alpha \in \sqrt{\nu(V \cap \mathbb{Z}^n)}$. The rest is obvious. □

Proposition 2.9. *Let $\mathcal{C} \subseteq \mathbb{Z}^n$ be a monoid and $V \subseteq \mathbb{R}^n$ be a vector subspace. If $\mathcal{C}$ is prismal, then the monoid $\mathcal{C} \cap V$ is prismal too.*

Let $\mathcal{C} \subseteq V$ and let V be defined over $\mathbb{Q}$. If $\nu\colon V \to \mathbb{R}^n$ is a linear embedding such that $\nu(V \cap \mathbb{Z}^n) \subseteq \mathbb{Z}^n$, then the monoid $\mathcal{C}$ is almost prismal if and only if the monoid $\nu(\mathcal{C})$ is almost prismal.

Proof. The first claim is obvious. Let now W be a vector subspace of $\mathbb{R}^n$. Set $U = \nu^{-1}(W) \subseteq V$. Then $\nu(\mathcal{C} \cap U) = \nu(\mathcal{C}) \cap \nu(U) = \nu(\mathcal{C}) \cap W$. By Lemma 2.8, we know that $\nu(V) \cap \mathbb{Z}^n = \sqrt{\nu(V \cap \mathbb{Z}^n)}$. Hence, we have

$$\begin{aligned}
\overline{\nu(\mathcal{C}) \cap W} &= \overline{\nu(\mathcal{C} \cap U)} = \mathbb{Z}^n \cap \overline{\operatorname{conv}(\nu(\mathcal{C} \cap U))}^{\mathbb{R}^n} \\
&= \nu(V) \cap \mathbb{Z}^n \cap \overline{\nu(\operatorname{conv}(\mathcal{C} \cap U))}^{\mathbb{R}^n} \\
&= \sqrt{\nu(V \cap \mathbb{Z}^n)} \cap \nu\big(\overline{\operatorname{conv}(\mathcal{C} \cap U)}^{\mathbb{R}^n}\big) \\
&= \sqrt{\nu(V \cap \mathbb{Z}^n)} \cap \sqrt{\nu\big(\overline{\operatorname{conv}(\mathcal{C} \cap U)}^{\mathbb{R}^n}\big)} \\
&= \sqrt{\nu\big(V \cap \mathbb{Z}^n \cap \overline{\operatorname{conv}(\mathcal{C} \cap U)}^{\mathbb{R}^n}\big)} \\
&= \sqrt{\nu(\overline{\mathcal{C} \cap U})} = \sqrt{\nu(\overline{\mathcal{C} \cap \nu^{-1}(W)})}.
\end{aligned}$$

Now, the monoid $\overline{\nu(\mathcal{C}) \cap W}$ is finitely generated if and only if $\sqrt{\nu(\overline{\mathcal{C} \cap \nu^{-1}(W)})}$ is so. And this happens if and only if the monoid $\overline{\mathcal{C} \cap \nu^{-1}(W)}$ is finitely generated, by Lemma 2.7 (i).

Therefore, $\nu(\mathcal{C})$ is almost prismal if and only if $\mathcal{C}$ is almost prismal. □

Theorem 2.10. *A cartesian product of prismal monoids is a prismal monoid.*

Proof. Let $\mathcal{C}_i$ be prismal monoids in $\mathbb{Z}^{d_i}$ for $i = 1, 2$. Then the monoid $\mathcal{C}_1 \times \mathcal{C}_2 \subseteq \mathbb{Z}^{d_1} \times \mathbb{Z}^{d_2}$ can be expressed as $\mathcal{C}_1 \times \mathcal{C}_2 = (\mathcal{C}_1 \times \mathbb{Z}^{d_2}) \cap (\mathbb{Z}^{d_1} \times \mathcal{C}_2)$. In view of Theorem 2.5, it is therefore enough to prove that $\mathcal{C} \times \mathbb{Z}$ is prismal whenever $\mathcal{C}$ is prismal.

Let $\mathcal{C} \subseteq \mathbb{Z}^n$ be a prismal monoid and let $\pi\colon \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ be the projection forgetting the last component. Let V be a subspace of $\mathbb{R}^n \times \mathbb{R}$. Due to Proposition 2.7(ii), we may consider that V is defined over $\mathbb{Q}$.

If $\ker(\pi) = \langle (0, 0, \dots, 0, 1)\rangle \subseteq V$, then $V = W \oplus \mathbb{R}$ for some subspace W of $\mathbb{R}^n \times \{0\}$. Therefore, we clearly obtain $\overline{V \cap (\mathcal{C} \times \mathbb{Z})} = \overline{(W \cap \mathcal{C}) \times \mathbb{Z}} = \overline{(W \cap \mathcal{C})} \times \mathbb{Z}$. Since $\mathcal{C}$ is prismal, $\overline{(W \cap \mathcal{C})}$ is a finitely generated monoid and the monoid $\overline{V \cap (\mathcal{C} \times \mathbb{Z})}$ is finitely generated as well.

Let now $\ker(\pi) \cap V = 0$. Set $\mathcal{C}' = V \cap (\mathcal{C} \times \mathbb{Z})$. By Proposition 2.9, the monoid $\mathcal{C}'$ is almost prismal if and only if the monoid $\pi(\mathcal{C}') = \pi(V) \cap \pi(\mathcal{C} \times \mathbb{Z}) = \pi(V) \cap \mathcal{C}$ is almost prismal. From the assumption we know that $\mathcal{C}$ is almost prismal, hence $\pi(V) \cap \mathcal{C}$ is so and, consequently, $\mathcal{C}'$ is prismal as well. In particular, $\overline{\mathcal{C}'} = \overline{V \cap (\mathcal{C} \times \mathbb{Z})}$ is finitely generated.

Finally, we have verified the conditions of prismality and the monoid $\mathcal{C} \times \mathbb{Z}$ is therefore prismal. □

Theorem 2.11. *Let $\pi\colon \mathbb{R}^n \to \mathbb{R}^k$ be a linear epimorphism such that $\pi(\mathbb{Z}^n) \subseteq \mathbb{Z}^k$. If a monoid $\mathcal{C} \subseteq \mathbb{Z}^k$ is almost prismal, then the monoid $(\pi_{|\mathbb{Z}^n})^{-1}(\mathcal{C})$ is almost prismal as well.*

Proof. First, assume that π is a canonical projection of the form $\pi(e_i) = e_i$ for $i = 1, \dots, k$ and $\pi(e_j) = 0$ for $j = k + 1, \dots, n$ (where e_i are the standard basis vectors). Then $(\pi_{|\mathbb{Z}^n})^{-1}(\mathcal{C}) = \mathcal{C} \times \mathbb{Z}^{n-k}$. By Theorem 2.10, this monoid is prismal, provided that $\mathcal{C}$ is prismal.

Further, let π be a scaling such that $n = k$ and $\pi(e_i) = k_i \cdot e_i$ for some $0 \neq k_i \in \mathbb{Z}$, $i = 1, \dots, n$. Clearly, $\sqrt{\pi(\mathbb{Z}^n)} = \mathbb{Z}^n$. Set $\widetilde{\mathcal{C}} = (\pi_{|\mathbb{Z}^n})^{-1}(\mathcal{C})$. Using Proposition 2.7 (i) and Lemma 2.8, we obtain that the monoid $\widetilde{\mathcal{C}}$ is almost prismal if and only if $\pi(\widetilde{\mathcal{C}})$ is almost prismal. This is equivalent to

$$\sqrt{\pi(\widetilde{\mathcal{C}})} = \sqrt{\pi((\pi_{|\mathbb{Z}^n})^{-1}(\mathcal{C}))} = \sqrt{\mathcal{C}}$$

being almost prismal, and that happens if and only if $\mathcal{C}$ is almost prismal. Since $\mathcal{C}$ is almost prismal, we have proved that the monoid $\widetilde{\mathcal{C}} = (\pi_{|\mathbb{Z}^n})^{-1}(\mathcal{C})$ is almost prismal too.

Finally, in the general case, we can consider that $\pi = \psi_1 \circ \nu \circ \tilde{\pi} \circ \psi_2$, where $\tilde{\pi}$ is a canonical projection, ν a scaling and $\psi_1(\psi_2$, resp.) corresponds to an isomorphism of the group $\mathbb{Z}^k$ ($\mathbb{Z}^n$, resp.). Now, combining all the cases together, we obtain that from the prismality of $\mathcal{C}$, it follows that $(\pi_{|\mathbb{Z}^n})^{-1}(\mathcal{C})$ is almost prismal, too. □

Now we will be interested in establishing a decomposition of a prismal monoid into faces. Let $K \subseteq \mathbb{R}^n$ be a convex set. A non-empty subset $A \subseteq K$ will be called a *relatively open face* of K if

- A is convex,
- $\mathrm{ri}(A) = A$,
- for every line segment $L \subseteq K$ such that $\mathrm{ri}(L) \cap A \neq \emptyset$, we have $\mathrm{ri}(L) \subseteq A$.

Theorem 2.12. *For every cone K in $\mathbb{R}^n$ there is a (unique) decomposition $\mathbf{K} = \{A_i \mid i \in I\}$ of K into a disjoint union of relatively open faces A_i of K, i.e., $K = \bigsqcup_{i \in I} A_i$.*

Moreover, let $A \in \mathbf{K}$ and let $x \in A$ and $y \in K \setminus \overline{A}^{\mathbb{R}^n}$. Then there is a relatively open face $B \in \mathbf{K}$ such that the relative interior of the line segment $\mathrm{conv}(\{x, y\})$ *lies in B and* $\dim(B) > \dim(A)$.

Proof. It is easy to verify that the following construction provides the desired decomposition. For every $x \in K$, there is a unique vector space W_x of maximal dimension such that x is a relatively inner point of the convex set $W_x \cap K$. Now, set a relation on K as $x \sim y$ if and only if $W_x = W_y$. This relation is an equivalence and the partition sets are the desired relatively open faces of K. In particular, such a face A is of the form $A = \mathrm{ri}(W_x \cap K)$, where $x \in A$. □

Finally, we are ready to prove the following result, which is the culmination of this section. The corollary establishes geometrical properties of prismal monoids that will play a key role later in the proof of Theorem 4.4. Its proof will go by downwards induction on the dimension of the face $\mathcal{D}$, and so we will need to be able to relate the properties of lower-dimensional faces to the higher-dimensional ones, as in part (iii) of the following corollary.

Corollary 2.13. *Let $\mathcal{C} \subseteq \mathbb{Z}^n$ be a prismal monoid. Let $K = \mathrm{conv}(\mathcal{C}) \subseteq \mathbb{R}^n$ and let $\mathbf{K}$ be the unique decomposition of K into relatively open faces. For a relatively open face $A \in \mathbf{K}$ of K let $A^0 = A \cup \{0\}$ be the cone arising from A.*

Set $\mathbf{D}(\mathcal{C}) := \{A^0 \cap \mathcal{C} \mid A \in \mathbf{K}\}$. Then $\mathbf{D}(\mathcal{C})$ is a decomposition of $\mathcal{C}$ into pure monoids (i.e., $\mathbf{D}(\mathcal{C}) = \bigcup_{\mathcal{D} \in \mathbf{D}(\mathcal{C})} \mathcal{D}$ and the union is "almost disjoint": $\mathcal{D} \cap \mathcal{D}' = \{0\}$ for $\mathcal{D} \neq \mathcal{D}'$) and for each $\mathcal{D} \in \mathbf{D}(\mathcal{C})$, the following hold:

(i) *The monoid $\overline{\mathcal{D}}$ is finitely generated.*

(ii) *If* $\dim(\mathcal{D}) = \dim(\mathcal{C})$, *then* $\overline{\mathcal{D}} = \overline{\mathcal{C}}$.

(iii) *For all* $0 \neq \alpha \in \mathcal{D}$ *and* $\beta \in \mathcal{C} \setminus \overline{\mathcal{D}}$, *there is* $\mathcal{E} \in \mathbf{D}(\mathcal{C})$ *such that* $\dim(\mathcal{E}) > \dim(\mathcal{D})$ *and* $\alpha + \beta \in \mathcal{E}$.

(iv) *For all* $0 \neq \alpha \in \mathcal{D}$ *and* $\gamma \in \overline{\mathcal{D}}$, *we have* $\alpha + \gamma \in \mathcal{D}$.

Proof. By the definition of the decomposition, we have $\mathcal{D} = A^0 \cap \mathcal{C}$, where $A = \mathrm{ri}(W \cap K)$ for some vector subspace $W \subseteq \mathbb{R}^n$ defined over $\mathbb{Q}$. Clearly, $\mathcal{D}$ is a pure monoid.

Further, we show that $\overline{\mathcal{D}} = \overline{W \cap \mathcal{C}} = \mathbb{Z}^n \cap \overline{A}^{\mathbb{R}^n}$. By the definition, we have

$$\overline{\mathcal{D}} = \mathbb{Z}^n \cap \overline{\mathrm{conv}(A^0 \cap \mathcal{C})}^{\mathbb{R}^n}$$

and

$$\overline{W \cap \mathcal{C}} = \mathbb{Z}^n \cap \overline{\mathrm{conv}(W \cap \mathcal{C})}^{\mathbb{R}^n}.$$

Since $W \subseteq \mathbb{R}^n$ is defined over $\mathbb{Q}$, there is a pure monoid $\mathcal{F} \subseteq \mathbb{Z}^n$ such that $W = \operatorname{conv}(\mathcal{F})$. Hence, by Proposition 2.3 (ii), we have

$$A = \operatorname{ri}(W \cap K) = \operatorname{ri}(\operatorname{conv}(\mathcal{F}) \cap \operatorname{conv}(\mathcal{C})) = \operatorname{ri}(\operatorname{conv}(\mathcal{F} \cap \mathcal{C})).$$

Therefore, there is a pure monoid $\mathcal{F}' \subseteq \mathbb{Z}^n$ such that $A^0 = A \cup \{0\} = \operatorname{conv}(\mathcal{F}')$. Now, by Proposition 2.2 (i) and Proposition 2.3 (ii) again, we obtain

$$\overline{\operatorname{conv}(A^0 \cap \mathcal{C})}^{\mathbb{R}^n} = \overline{A^0 \cap \operatorname{conv}(\mathcal{C})}^{\mathbb{R}^n} = \overline{A}^{\mathbb{R}^n} = \overline{\operatorname{ri}(W \cap K)}^{\mathbb{R}^n} = \overline{W \cap K}^{\mathbb{R}^n} = \overline{\operatorname{conv}(W \cap \mathcal{C})}^{\mathbb{R}^n}.$$

It follows that $\overline{\mathcal{D}} = \overline{W \cap \mathcal{C}} = \mathbb{Z}^n \cap \overline{A}^{\mathbb{R}^n}$.

Now we can prove the claims of the statement.

(i) Since $\mathcal{C}$ is prismal, $\overline{\mathcal{D}} = \overline{W \cap \mathcal{C}}$ is a finitely generated monoid.

(ii) If $\dim(\mathcal{D}) = \dim(K)$, then $\mathcal{D} = A^0 \cap \mathcal{C}$, where $A = \operatorname{ri}(K)$ and $W = \langle \mathcal{C} \rangle$. By the preliminary part of the proof and by Proposition 2.2 (i), we have $\overline{\mathcal{D}} = \mathbb{Z}^n \cap \overline{A}^{\mathbb{R}^n} = \mathbb{Z}^n \cap \overline{K}^{\mathbb{R}^n} = \overline{\mathcal{C}}$.

(iii) Let $0 \neq \alpha \in \mathcal{D}$ and $\beta \in \mathcal{C} \setminus \overline{\mathcal{D}}$. Since $\overline{\mathcal{D}} = \mathbb{Z}^n \cap \overline{A}^{\mathbb{R}^n}$, we have $\beta \in K \setminus \overline{A}^{\mathbb{R}^n}$. The rest follows immediately from Theorem 2.12 and from the fact that $\mathcal{C}$ is pure.

(iv) First note that, by Proposition 2.3 (i), we have

$$\mathcal{D} = \mathcal{C} \cap A^0 = \mathbb{Z}^n \cap \operatorname{conv}(\mathcal{C}) \cap A^0 = \mathbb{Z}^n \cap A^0.$$

Now, let $0 \neq \alpha \in \mathcal{D}$ and $\gamma \in \overline{\mathcal{D}} = \mathbb{Z}^n \cap \overline{A}^{\mathbb{R}^n}$. Then $\alpha \in \operatorname{ri}(A) = A$ is an inner point of a convex set A and $\gamma \in \overline{A}^{\mathbb{R}^n}$. Since A^0 is a cone, we therefore have $\alpha + \gamma \in A^0 \cap \mathbb{Z}^n = \mathcal{D}$. □

3 Every monoid associated to a finite tuple of semiring-generators of a parasemifield is prismal

Let now S be a parasemifield. We use the canonical pre-order $\leq_S$ defined as $a \leq_S b$ if and only if $a = b$ or there exists $c \in S$ such that $a + c = b$; it is in fact an order (see, e.g., [35, Section 2]). Note that it is preserved by addition, multiplication and anti-preserved by inversion in S (i.e., $a \leq_S b$ implies $a^{-1} \geq_S b^{-1}$ for all $a, b \in S$).

Let A be the *prime* subparasemifield of S, i.e., the smallest (possibly trivial) parasemifield contained in S. There are only two possibilities for A: either it is isomorphic to $\mathbb{Q}^+$, or it is trivial (i.e., it consists of a single element).

Let us now introduce the set Q_S of all elements that are smaller than some element of A. As was already noticed in [18, 22], using Q_S, one can define a monoid $\mathcal{C}_X(S)$ which plays a key role in the proofs.

The set

$$Q_S := \{a \in S \mid \text{there exists } q \in A \text{ such that } a \leq_S q\}$$

is a subsemiring of S. Clearly, for every $a, b \in S$ such that $a + b \in Q_S$, we have that $a, b \in Q_S$.

We say that an n-tuple $X = (x_1, \dots, x_n)$, where $x_i \in S$ for $i = 1, \dots, n$, is *a generating tuple of S (considered as a semiring)* if

$$S = \{f(x_1, \dots, x_n) \mid 0 \neq f \in \mathbb{N}[T_1, \dots, T_n]\},$$

where $\mathbb{N}[T_1, \dots, T_n]$ is the semiring of polynomials over the variables $T_1, \dots, T_n$ with non-negative integer coefficients.

Let X be such a generating tuple. For $\alpha = (a_1, \dots, a_n) \in \mathbb{N}_0^n$, we put

$$\boldsymbol{x}^\alpha := x_1^{a_1} \dots x_n^{a_n}$$

and we denote by

$$\mathcal{C}_X(S) := \{\alpha \in \mathbb{N}_0^n \mid \boldsymbol{x}^\alpha \in Q_S\}$$

the *corresponding monoid* assigned to X and S.

Obviously, $\mathcal{C}_X(S)$ is a submonoid of $(\mathbb{N}_0^n, +)$ and the semiring Q_S is generated by the set $\{\boldsymbol{x}^\alpha \mid \alpha \in \mathcal{C}_X(S)\}$.

The goal of this section is to study the monoid $\mathcal{C}_X(S)$ and to show its prismality. The following two results establish some basic geometrical information about $\mathcal{C}_X(S)$. They were already used in [18, 22], but we include their short proofs for the sake of completeness.

Proposition 3.1 ([22, Lemma 4.6]). *If $a \in S$ and $n \in \mathbb{N}$ are such that $a^n \in Q_S$, then $a \in Q_S$.*

Proof. Let A be the prime parasemifield of S. If $a^n \in Q_S$, then, clearly, there are $u \in S$ and $q \in A$ such that $a^n + u = q^n$. Set $w = q^{n-1} + q^{n-2}a + \cdots + qa^{n-2} + a^{n-1}$. Then we have

$$\begin{aligned} aw + u &= q^{n-1}a + q^{n-2}a^2 + \cdots + qa^{n-1} + a^n + u \\ &= q^{n-1}a + q^{n-2}a^2 + \cdots + qa^{n-1} + q^n \\ &= qw. \end{aligned}$$

Now, $a + uw^{-1} = q \in A$, and therefore $a \in Q_S$. □

Corollary 3.2. *Let $X = (x_1, \ldots, x_n)$ be a generating tuple for a parasemifield S (as a semiring). Then the associated monoid $\mathcal{C}_X(S)$ is pure.*

In order to show the prismality of $\mathcal{C}_X(S)$, we need to first recall the classification of additively idempotent parasemifields, finitely generated as semirings [20].

Definition 3.3. Let us recall the notion of a rooted tree and an ℓ-group (additively idempotent parasemifield, resp.) that is associated to it (for an explicit description with more details, see [20, beginning of Section 4]).

First note that to each lattice-ordered commutative group (an ℓ-group for short) $G(\oplus, \vee, \wedge)$ corresponds an additively idempotent parasemifield $G(\vee, \oplus)$, and that to describe the infimum and supremum operations $\wedge, \vee$ in an ℓ-group G, it suffices to describe the corresponding ordering $\leq_G$.

A *rooted tree* (T, v_0) is a (finite, non-oriented) connected graph T containing no cycles and having a specified vertex, the root v_0.

Attach a copy of the group of integers $\mathbb{Z} = \mathbb{Z}_w$ to each vertex w of T. The ℓ-group $G(T, v_0)$ associated to (T, v_0) is an additive group that arises as a direct product of these groups. It remains to describe the partial order on $G(T, v_0)$. Let e_w be the generator of the direct summand $\mathbb{Z}_w$. The ordering $\leq_{G(T,v_0)}$ on $G(T, v_0)$ can be expressed as follows.

Consider (T, v_0) as a partially ordered set with the greatest element v_0 where the ordering $\preceq_{(T,v_0)}$ is given by the graph T that is considered as a Hasse diagram oriented downwards.

First, assume that T is a chain. Then $\leq_{G(T,v_0)}$ is defined as the lexicographical ordering on $G(T, v_0)$ induced by the linear ordering $\preceq_{(T,v_0)}$ on T.

Now, consider the general case of a rooted tree. Then for $a, b \in G(T, v_0)$, set $a \leq_{G(T,v_0)} b$ if and only if $a \leq_{G(\tilde{T},v_0)} b$ for all possible extensions of T into a chain $\tilde{T}$ with the same underlying set of vertices.

By the well-known correspondence of ℓ-groups and commutative additively idempotent parasemifields, $G(T, v_0)$ can be treated as an additively idempotent parasemifield and $\leq_{G(T,v_0)}$ is the natural ordering on this parasemifield (for example, see [36, 37]).

Proposition 3.4. *Let (T, v_0) be a rooted tree and $S = G(T, v_0)$ be the additively idempotent parasemifield corresponding to it. Let e_w have the same meaning as in Definition 3.3 and let X be a tuple of canonical generators of the parasemifield S considered as a semiring, i.e., $X = (e_{w_1}, -e_{w_1}, \ldots, e_{w_n}, -e_{w_n})$, where $w_1, \ldots, w_n$ are all the pairwise different vertices of the graph T. Then the associated monoid $\mathcal{C}_X(S)$ is prismal.*

Proof. First, assume that the rooted tree is a chain. In this case, we see that S is a parasemifield corresponding to an ℓ-group $(\mathbb{Z}^n, +)$ with the usual lexicographical ordering $\leq_{\text{lex}}$. In this case the canonical tuple is of the form $X = (e_1, -e_1, \ldots, e_n, -e_n)$, where $e_i \in \mathbb{Z}^n$ are the usual vectors of the standard basis (i.e., $e_1 = (1, 0, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, etc.).

As the next step we show that the monoid $\mathcal{D}_n = \{\alpha \in \mathbb{Z}^n \mid \alpha \leq_{\text{lex}} 0\}$ is prismal. Clearly, the monoid $\mathcal{D}_n$ is pure. Now, we proceed by induction on $n \geq 1$. The case $n = 1$ is obvious. For the induction step, choose a vector subspace W of $\mathbb{R}^n$. Due to Proposition 2.7 (ii), we may consider that W is defined over $\mathbb{Q}$. If $W \not\subseteq \{0\} \times \mathbb{R}^{n-1}$, then $\overline{\mathcal{D}_n \cap W} = \{(a_1, \dots, a_n) \in W \cap \mathbb{Z}^n \mid a_1 \geq 0\}$ and if $W \subseteq \{0\} \times \mathbb{R}^{n-1}$, then $\overline{\mathcal{D}_n \cap W} = \overline{(\{0\} \times \mathcal{D}_{n-1}) \cap W}$. The induction step now follows easily and the monoid $\mathcal{D}_n$ is therefore prismal.

Now,

$$\mathcal{C}_X(S) = \{(a_1, b_1, \dots, a_n, b_n) \in \mathbb{N}_0^{2n} \mid (a_1 - b_1, \dots, a_n - b_n) \in \mathcal{D}_n\}.$$

In other words, $\mathcal{C}_X(S) = \mathbb{N}_0^{2n} \cap (\pi_{|\mathbb{Z}^{2n}})^{-1}(\mathcal{D}_n)$, where

$$\pi\colon \mathbb{R}^{2n} \to \mathbb{R}^n, \quad \pi(a_1, b_1, \dots, a_n, b_n) = (a_1 - b_1, \dots, a_n - b_n).$$

By Theorems 2.5, 2.11 and Corollary 3.2, it follows that $\mathcal{C}_X(S)$ is prismal.

In the case of a general rooted tree, we obtain by the definition of $\leq_{G(T,v_0)}$ that

$$\mathcal{C}_X(G(T, v_0)) = \bigcap \{\mathcal{C}_X(G(\widetilde{T}, v_0)) \mid \widetilde{T} \text{ extends } T \text{ to a chain}\}.$$

The monoid $\mathcal{C}_X(G(T, v_0))$ is therefore an intersection of prismal monoids (according to the first part of the proof) and thus, by Theorem 2.5, $\mathcal{C}_X(G(T, v_0))$ is prismal as well. □

Theorem 3.5 ([20, Theorem 4.1]). *Let S be an additively idempotent parasemifield, finitely generated as a semiring. Then S is a (finite) product of parasemifields of the form $G(T_i, v_i)$, where (T_i, v_i) are rooted trees and $G(T_i, v_i)$ are associated additively idempotent parasemifields (or equivalently ℓ-groups).*

Hence, we explicitly understand the structure of additively idempotent parasemifields and of the corresponding monoids $\mathcal{C}_X(S)$ (by Proposition 3.4). Given a general parasemifield, we will now show that its monoid is in fact the same as the monoid of some additively idempotent parasemifield.

Proposition 3.6. *Define a congruence $\sim$ on S by $x \sim y$ if and only if $xy^{-1} \in Q_S$ and $yx^{-1} \in Q_S$ for $x, y \in S$. Then $U = S_{/\sim}$ is the largest factor-parasemifield of S that is additively idempotent.*

If S is generated by a tuple $X = (x_1, \dots, x_n)$ as a semiring, then U is generated as a semiring by the corresponding tuple $X' = (x'_1, \dots, x'_n)$, where $x'_i = x_{i_{/\sim}}$, and $\mathcal{C}_X(S) = \mathcal{C}_{X'}(U)$.

Proof. First, we show that the relation $\sim$ is indeed a congruence of the parasemifield S. The only property that does not seem to be obvious is that $x \sim y$ implies $x + a \sim y + a$ for every $x, y, a \in S$. Assume therefore that $x \sim y$. Then $xy^{-1} \in Q_S$ and, consequently, there is q in the prime subparasemifield A such that $x \leq_S qy$. We can assume without loss of generality that $1 \leq_S q$. Hence, $x + a \leq_S qy + a \leq_S qy + qa = q(y + a)$ for every $a \in S$. We obtain that $(x + a)(y + a)^{-1} \in Q_S$ and similarly $(y + a)(x + a)^{-1} \in Q_S$. The relation $\sim$ is therefore indeed a congruence.

Further, since $x(2x)^{-1} = 2^{-1} \in Q_S$ and $2x(x)^{-1} = 2 \in Q_S$, we have $x \sim 2x$. Therefore, $U = S_{/\sim}$ is an additively idempotent parasemifield. It remains to prove maximality. Let $\varphi\colon S \to T$ be a parasemifield homomorphism such that T is additively idempotent. If we have $x \sim y$, then, as before, we know that $x \leq_S qy$ for some $q \in A$. Hence, $\varphi(x) \leq_T \varphi(q)\varphi(y) = \varphi(y)$ and, similarly, $\varphi(y) \leq_T \varphi(x)$. As the relation $\leq_T$ is an order in the additively idempotent parasemifield T, we get that $\varphi(x) = \varphi(y)$. This means that $U = S_{/\sim}$ is the largest factor-parasemifield of S which is additively idempotent.

Finally, let S be generated by a tuple $X = (x_1, \dots, x_n)$ as a semiring. Let $\pi\colon S \to U = S_{/\sim}$ be the natural epimorphism. Clearly, U is generated by the corresponding tuple $X' = (x'_1, \dots, x'_n)$, where $x'_i = \pi(x_i)$. Since U is additively idempotent, $\pi(A)$ is the prime subparasemifield of $U = \pi(S)$.

Let $\alpha \in \mathcal{C}_X(S)$. Then $\boldsymbol{x}^\alpha \in Q_S$ and therefore we have $(\boldsymbol{x}')^\alpha = \pi(\boldsymbol{x}^\alpha) \in \pi(Q_S) \subseteq Q_U$. We have obtained that $\mathcal{C}_X(S) \subseteq \mathcal{C}_{X'}(U)$.

Let, on the other hand, be $\alpha \in \mathcal{C}_{X'}(U)$. Then $\pi(\boldsymbol{x}^\alpha) = (\boldsymbol{x}')^\alpha \leq_U 1_U = \pi(1_S)$. Hence, there is $b \in S$ such that $\pi(\boldsymbol{x}^\alpha) + \pi(b) = \pi(1_S)$. It follows that $\boldsymbol{x}^\alpha + b \sim 1_S$ and there is $q \in A$ such that $\boldsymbol{x}^\alpha + b \leq q \cdot 1_S = q$. Thus, $\boldsymbol{x}^\alpha \in Q_S$ and $\alpha \in \mathcal{C}_{X'}(U)$. We have shown that $\mathcal{C}_{X'}(U) \subseteq \mathcal{C}_X(S)$.

Altogether we have proved that $\mathcal{C}_{X'}(U) = \mathcal{C}_X(S)$. □

Finally, it remains to deal with the dependence of $\mathcal{C}_X(S)$ on the generating tuple X. We start with an easy lemma.

Lemma 3.7. *Let $X = (x_1, \dots, x_n)$ be a generating tuple for S such that the monoid $\mathcal{C}_X(S)$ is prismal. Then for the generating tuple $Y = (x_1, \dots, x_n, x_1)$, the monoid $\mathcal{C}_Y(S)$ is prismal as well.*

Proof. Clearly, $\alpha = (a_1, \dots, a_n, a_{n+1}) \in \mathcal{C}_Y(S) \subseteq \mathbb{R}^{n+1}$ if and only if

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} x_1^{a_{n+1}} = x_1^{a_1+a_{n+1}} x_2^{a_2} \cdots x_n^{a_n} \in Q,$$

and this is equivalent to $(a_1 + a_{n+1}, a_2, \dots, a_n) \in \mathcal{C}_X(S) \subseteq \mathbb{R}^n$. Set $\pi\colon \mathbb{R}^{n+1} \to \mathbb{R}^n$ as

$$\pi(a_1, \dots, a_{n+1}) = (a_1 + a_{n+1}, a_2, \dots, a_n).$$

Then, by Theorems 2.5 and 2.11, $\mathcal{C}_Y(S) = \mathbb{N}_0^{n+1} \cap (\pi_{|\mathbb{Z}^{n+1}})^{-1}(\mathcal{C}_X(S))$ is prismal. □

Now we are ready to prove everything together and to show the main result of this section.

Theorem 3.8. *Let $X = (x_1, \dots, x_n)$ be a generating tuple for a parasemifield S (as a semiring). Then the associated monoid $\mathcal{C}_X(S)$ is prismal.*

Proof. First we show that if S is additively idempotent and finitely generated as a semiring, then there is a tuple $Y = (y_1, \dots, y_k)$ of length at least two (i.e., $k \geq 2$) such that

- $y_1 y_2 = 1_S$,
- the tuple Y generates S by using only the multiplication,
- the associated monoid $\mathcal{C}_Y(S)$ is prismal.

First of all, assume that $S = G(T, v)$ for some rooted tree (T, v). Then the monoid associated to the canonical generating tuple Y is prismal, by Proposition 3.4. Clearly, the tuple Y generates S using only multiplication (the corresponding ℓ-group is generated by the tuple Y only as a semigroup without using the inverse and infimum or supremum operations). In the case that S is trivial, we can set $Y = (1_S, 1_S)$.

Now, if S is an arbitrary additively idempotent parasemifield, then S is a finite product of parasemifields $S_i = G(T_i, v_i)$, by Theorem 3.5. If Y_i are the corresponding canonical generating tuple of S_i and we put $Y = \cup_i Y_i$ (i.e., the tuples are simply concatenated in some order), then Y generates S multiplicatively and $\mathcal{C}_Y(S) = \prod_i \mathcal{C}_{Y_i}(S_i)$. Since all the monoids $\mathcal{C}_{Y_i}(S_i)$ are prismal, the monoid $\mathcal{C}_Y(S)$ is prismal as well, by Theorem 2.10.

Further, we proceed with the general case of a parasemifield S generated by the tuple $X = (x_1, \dots, x_n)$ as a semiring. By Corollary 3.2, the associated monoid $\mathcal{C}_X(S)$ is pure. As in Proposition 3.6, let U be the largest factor-parasemifield of S which is additively idempotent and let $X' = (x'_1, \dots, x'_n)$ be the corresponding generating tuple of U. By Proposition 3.6, we know that $\mathcal{C}_X(S) = \mathcal{C}_{X'}(U) \subseteq \mathbb{N}_0^n$.

By the previous part of the proof, there is a tuple $Y = (y_1, \dots, y_k) \subseteq U$ that generates U multiplicatively, $y_1 y_2 = 1_U$ and $\mathcal{C}_Y(U)$ is prismal. The elements of X' may be expressed as monomials in Y, i.e., there is a $k \times n$ matrix $\mathbb{A} = (a_{i,j})$ with non-negative integer entries such that $x'_j = \prod_{i=1}^k y_i^{a_{i,j}}$ for every $j = 1, \dots, n$. Clearly, for $\alpha = (a_1, \dots, a_n)^T \in \mathbb{N}_0^n$, we have $\alpha \in \mathcal{C}_{X'}(U)$ if and only if $\mathbb{A}\alpha \in \mathcal{C}_Y(U)$. Let $\nu\colon \mathbb{R}^n \to \mathbb{R}^k$ be a linear map corresponding to the matrix $\mathbb{A}$. Clearly, $\mathcal{C}_{X'}(U) = \nu^{-1}(\mathcal{C}_Y(U))$.

We can assume without loss of generality that ν is an embedding. If this is not the case, then some column (let us say the j_0-th column for $j_0 \in \{1, \dots, n\}$) is linearly dependent on the other columns. Let Y' be a generating tuple obtained from Y by doubling the element y_1, i.e., $Y' = (y_1, \dots, y_k, y_1)$. Since $x'_{j_0} = (\prod_{i=1}^k y_i^{a_{i,j}}) \cdot (y_1 y_2)$, we can set

$$a'_{i,j} = \begin{cases} a_{2,j_0} + 1 & \text{if } i = 2 \text{ and } j = j_0, \\ 1 & \text{if } i = k+1 \text{ and } j = j_0, \\ 0 & \text{if } i = k+1 \text{ and } j \neq j_0, \\ a_{i,j} & \text{otherwise,} \end{cases}$$

and the $(k+1) \times n$ matrix $\mathbb{A}' = (a'_{i,j})$ expresses elements from X' with the help of Y' in a similar manner as before. The j_0-th column of $\mathbb{A}'$ is now independent on the others. We can repeat this process until we arrive at a matrix with rank n.

Now, the linear map $\nu\colon \mathbb{R}^n \to \mathbb{R}^k$ is an embedding and $\nu(\mathbb{Z}^n) \subseteq \mathbb{Z}^k$. Therefore, by Proposition 2.9, $\mathcal{C}_{X'}(U) = \nu^{-1}(\mathcal{C}_Y(U))$ is prismal if and only if $\nu(\mathcal{C}_{X'}(U)) = \mathcal{C}_Y(U) \cap \operatorname{Im}(\nu)$ is prismal. Finally, since we know that $\mathcal{C}_Y(U)$ is prismal, it follows that $\mathcal{C}_{X'}(U)(= \mathcal{C}_X(S))$ is prismal as well. Therefore, any monoid associated to any tuple, that generates a parasemifield as a semiring, is prismal. □

4 Every parasemifield that is finitely generated as a semiring is additively idempotent

For a semiring T, the *Grothendieck ring* $G(T)$ is defined in the same way as the Grothendieck group is defined for a (commutative) semigroup. Namely, on the set $\widetilde{T} = T \times T$, we define the operations $\oplus$ and $\odot$ as

$$(x, y) \oplus (x', y') = (x + x', y + y'),$$
$$(x, y) \odot (x', y') = (xx' + yy', xy' + x'y),$$

and a relation $\approx$ as

$$(x, y) \approx (x', y') \iff \text{there exists } t \in T \text{ such that } x + y' + t = x' + y + t$$

for every $x, x', y, y' \in T$. Now $\approx$ is a congruence on the semiring $(\widetilde{T}, \oplus, \odot)$ and $G(T) = \widetilde{T}_{/\approx}$. For an element $x \in T$, denote by $[x]$ the corresponding element in $G(T)$, i.e., we have a semiring homomorphisms $T \to G(T)$, defined as $x \mapsto [x]$.

The motivation behind the definition of $G(T)$ is that we would like to work with the difference ring $T - T$. Unfortunately, if T is not additively cancellative, $T - T$ is not well defined. To remedy this, one usually considers the Grothendieck ring $G(T)$ as defined above with the understanding that $(x, y)_{/\approx} \in G(T)$ should correspond to the difference $[x] - [y]$.

Finally, note that for an element $u \in T$, we have that $[u] = 0$ in $G(T)$ if and only if $z = u + z$ for some element $z \in T$. We will use this easy observation several times in this section, especially in the proof of Theorem 4.4.

Theorem 4.1. *The parasemifield S is additively idempotent if and only if the Grothendieck ring $G(Q_S)$ is trivial.*

Proof. If S is additively idempotent, then Q_S is additively idempotent as well and therefore the Grothendieck ring $G(Q_S)$ has to be trivial.

For the opposite implication, assume that $G(Q_S)$ is trivial. Then there is $t \in Q_S$ such that $t = 1 + t$. By the definition of Q_S, there are $u \in A$ and $s \in S$ such that $t + s = u$. Therefore, we obtain $u = 1 + u$. This is a nontrivial equality within the prime subparasemifield A. It follows that A can not be isomorphic to $\mathbb{Q}^+$ (that is additively cancellative) and, therefore, A is trivial. This means that S is additively idempotent. □

Let $X = (x_1, \ldots, x_n)$ be a tuple that generates a parasemifield S as a semiring. Let $\mathcal{M} \subseteq \mathbb{N}_0^n$ be a subset. Denote by $S_X(\mathcal{M})$ the additive subsemigroup of $S(+)$ that is generated by the set $\{\boldsymbol{x}^\alpha \mid \alpha \in \mathcal{M}\}$ – recall that $\boldsymbol{x}^\alpha := x_1^{a_1} \cdots x_n^{a_n}$ if $\alpha = (a_1, \ldots, a_n)$.

Note that if $\mathcal{M}$ is a submonoid of $\mathbb{N}_0^n(+)$, then $S_X(\mathcal{M})$ is a semiring.

Lemma 4.2. *Let $X = (x_1, \ldots, x_n)$ be a tuple that generates a parasemifield S as a semiring. Let $\mathcal{C} = \mathcal{C}_X(S)$ and $\mathbf{D}(\mathcal{C})$ be the decomposition of $\mathcal{C}$ into monoids as in Corollary* 2.13.

Then for every $\mathcal{D} \in \mathbf{D}(\mathcal{C})$ and every $0 \neq \alpha \in \mathcal{D}$, the following hold:

(i) *If $u \in S_X(\mathcal{C} + \overline{\mathcal{D}})$, then $\boldsymbol{x}^\alpha u \in S_X(\mathcal{C}) = Q_S$.*

(ii) *If $u \in Q_S = S_X(\mathcal{C})$, then $\boldsymbol{x}^\alpha u \in S_X(\mathcal{F})$, where*

$$\mathcal{F} = \overline{\mathcal{D}} \cup \bigcup \{\mathcal{E} \in \mathbf{D}(\mathcal{C}) \mid \dim(\mathcal{E}) > \dim(\mathcal{D})\}.$$

Proof. (i) The element u is a sum of elements of the form $\boldsymbol{x}^{\gamma+\beta}$, where $\gamma \in \overline{\mathcal{D}}$ and $\beta \in \mathcal{C}$. By Corollary 2.13 (iv), we have $\alpha + \gamma \in \mathcal{D} \subseteq \mathcal{C}$. Therefore, we obtain that $\boldsymbol{x}^\alpha u \in S_X(\mathcal{C}) = Q_S$.

(ii) The element u is a sum of elements of the form $\boldsymbol{x}^\beta$, where $\beta \in \mathcal{C}$. Clearly, for $\beta \in \mathcal{C} \cap \overline{\mathcal{D}}$, we have $\alpha + \beta \in \overline{\mathcal{D}} \subseteq \mathcal{F}$ and therefore $\boldsymbol{x}^{\alpha+\beta} \in S_X(\mathcal{F})$. If $\beta \in \mathcal{C} \setminus \overline{\mathcal{D}}$, then, by Corollary 2.13 (iii), there is $\mathcal{E} \in \mathbf{D}(\mathcal{C})$ such that $\dim(\mathcal{E}) > \dim(\mathcal{D})$ and $\alpha + \beta \in \mathcal{E} \subseteq \mathcal{F}$. Hence, $\boldsymbol{x}^{\alpha+\beta} \in S_X(\mathcal{F})$.

Summing this up, we obtain that $\boldsymbol{x}^\alpha u \in S_X(\mathcal{F})$. □

For a ring R, let $\mathcal{N}(R) = \{a \in R \mid \text{there exists } \ell \in \mathbb{N} \text{ such that } a^\ell = 0\}$ denote the *nilradical of* R.

Remark 4.3. In a semiring T, an element $a \in T$ is called *additively divisible* if for every $m \in \mathbb{N}$, there is $b_m \in T$ such that $a = m \cdot b_m$.

Let us recall that in a finitely generated commutative ring R, any additively divisible element $a \in R$ has to be trivial (see, e.g., [25, Examples 1]).

Note that since the prime subparasemifield A of any parasemifield S is either trivial or isomorphic to the positive rationals $\mathbb{Q}^+$, it is obvious that A is additively divisible. It follows that every parasemifield S is additively divisible. Likewise, each subsemiring Q of S containing A is additively divisible; in particular, 1_S is additively divisible in Q_S.

Theorem 4.4. *Let $X = (x_1, \dots, x_n)$ be a tuple that generates a parasemifield S as a semiring. Then for every $0 \neq \alpha \in \mathcal{C}_X(S)$, the element $[\boldsymbol{x}^\alpha]$ is nilpotent in $G(Q_S)$.*

Proof. By Theorem 3.8, the monoid $\mathcal{C} := \mathcal{C}_X(S)$ is prismal. Let $\mathbf{D}(\mathcal{C})$ be the decomposition of $\mathcal{C}$ into monoids as in Corollary 2.13. Every non-zero element $\alpha \in \mathcal{C}$ belongs into precisely one monoid $\mathcal{D} \in \mathbf{D}(\mathcal{C})$. That is why we prove our assertion by the downward induction on the dimension of monoids $\mathcal{D}$ in $\mathbf{D}(\mathcal{C})$, i.e., from the highest dimension $n_0 = \dim(\mathcal{C})$ to the lowest one appearing in $\mathbf{D}(\mathcal{C})$.

We start with $n_0 = \dim(\mathcal{C})$. Let $\mathcal{D} \in \mathbf{D}(\mathcal{C})$ have the dimension n_0. By Corollary 2.13 (i)–(ii), the monoid $\overline{\mathcal{D}}$ is finitely generated and $\mathcal{C} \subseteq \overline{\mathcal{D}}$. It follows that the semiring $Q' = S_X(\overline{\mathcal{D}})$ is finitely generated and 1_S is an additively divisible element in Q' (as discussed in Remark 4.3). The ring $G(Q')$ has these properties as well and therefore, by Remark 4.3, it must be trivial. Hence, $z = 1_S + z$ in Q' for some $z \in Q'$.

Now, pick $0 \neq \alpha \in \mathcal{D}$. We have $\boldsymbol{x}^\alpha z = \boldsymbol{x}^\alpha + \boldsymbol{x}^\alpha z$. By Lemma 4.2 (i), we obtain that $\boldsymbol{x}^\alpha z \in Q_S$ and therefore $[\boldsymbol{x}^\alpha] = 0$ in $G(Q_S)$. In particular, $[\boldsymbol{x}^\alpha]$ is nilpotent in $G(Q_S)$.

For the induction step, assume that for the monoid $\mathcal{D} \in \mathbf{D}(\mathcal{C})$, we have that every element $[\boldsymbol{x}^\delta]$ is nilpotent in $G(Q_S)$ whenever the non-zero exponent $\delta \in \mathcal{C}$ lies in a monoid from $\mathbf{D}(\mathcal{C})$ of a bigger dimension than $\dim(\mathcal{D})$. Let us still denote a few auxiliary structures.

- Denote by $Q'' = S_X(\mathcal{C} + \overline{\mathcal{D}})$ the corresponding subsemiring of S.
- For an element $u \in Q''$, we denote by $[\![u]\!]$ the corresponding element in $G(Q'')$ to distinguish it from the notation of analogous elements $[a] \in G(Q_S)$ with $a \in Q_S$.
- Denote by $R = {}^{G(Q'')}/_{\mathcal{N}(G(Q''))}$ the quotient ring of $G(Q'')$ by its nilradical.
- Let $\pi\colon G(Q'') \to R$ be the natural ring epimorphism.
- Let T be the subring of R generated by the set $\{\pi([\![\boldsymbol{x}^\beta]\!]) \mid \beta \in \overline{\mathcal{D}}\}$.

By Corollary 2.13 (i), the monoid $\overline{\mathcal{D}}$ is finitely generated and therefore the ring T is finitely generated as well.

Now, pick $0 \neq \alpha \in \mathcal{D}$. Again, the element 1_S is divisible in Q_S, by Remark 4.3. Therefore, we have a set of equalities $1_S = m \cdot z_m$, $m \in \mathbb{N}$, where $z_m \in Q_S$. It follows that $\boldsymbol{x}^\alpha = m \cdot \boldsymbol{x}^\alpha z_m$.

Further, let us show that $\pi([\![\boldsymbol{x}^\alpha z_m]\!]) \in T$. By Lemma 4.2 (ii), the element $\boldsymbol{x}^\alpha z_m$ is a sum of elements of the form $\boldsymbol{x}^\beta$, where either $\beta \in \overline{\mathcal{D}}$ or $\beta \in \mathcal{E}$ for some monoid $\mathcal{E} \in \mathbf{D}(\mathcal{C})$ such that $\dim(\mathcal{E}) > \dim(\mathcal{D})$. In the first case, we clearly have that $\pi([\![\boldsymbol{x}^\beta]\!]) \in T$. Let us therefore assume the latter case of β. Then, by the induction hypothesis, $[\boldsymbol{x}^\beta]$ is a nilpotent element in $G(Q_S)$. Since $Q_S \subseteq Q''$, there is a natural ring homomorphism $G(Q_S) \to G(Q'')$, and it follows that $[\![\boldsymbol{x}^\beta]\!]$ is a nilpotent element in $G(Q'')$ as well. Therefore, $\pi([\![\boldsymbol{x}^\beta]\!]) = 0$ in R. In particular, $\pi([\![\boldsymbol{x}^\beta]\!]) = 0 \in T$. Summing this up, we have proved that $\pi([\![\boldsymbol{x}^\alpha z_m]\!]) \in T$.

Finally, as we have $\pi([\![\boldsymbol{x}^\alpha z_m]\!]) \in T$ and $\pi([\![\boldsymbol{x}^\alpha]\!]) = m \cdot \pi([\![\boldsymbol{x}^\alpha z_m]\!])$ for every $m \in \mathbb{N}$, the element $\pi([\![\boldsymbol{x}^\alpha]\!]) \in T$ is now additively divisible in the finitely generated ring T. By Remark 4.3, it follows that $\pi([\![\boldsymbol{x}^\alpha]\!]) = 0$ in T and, of course, the same is true in $R = {}^{G(Q'')}/_{\mathcal{N}(G(Q''))}$. Hence, there is $k \in \mathbb{N}$ such that $[\![\boldsymbol{x}^{k\alpha}]\!] = 0$ in $G(Q'')$. Therefore, there is $u \in Q''$ such that $u = \boldsymbol{x}^{k\alpha} + u$. Multiplying this equality by $\boldsymbol{x}^\alpha$, we obtain that $\boldsymbol{x}^\alpha u = \boldsymbol{x}^{(k+1)\alpha} + \boldsymbol{x}^\alpha u$. By Lemma 4.2 (i), it follows that $\boldsymbol{x}^\alpha u \in Q_S$. This means that $[\boldsymbol{x}^{(k+1)\alpha}] = 0$ in $G(Q_S)$. In other words, $[\boldsymbol{x}^\alpha]$ is nilpotent in $G(Q_S)$.

This concludes our proof and, indeed, for every $0 \neq \alpha \in \mathcal{C}_X(S)$ the element $[\boldsymbol{x}^\alpha]$ is nilpotent in $G(Q_S)$. □

Theorem 4.5. *Every parasemifield that is finitely generated as a semiring is additively idempotent.*

Proof. We can assume without loss of generality that the unity 1_S is one of the generators $x_1, \dots, x_n$, in particular, $x_1 = 1_S$. By Theorem 4.4, the element $x_1 = 1_S$ is nilpotent in $G(Q_S)$. This implies that $G(Q_S)$ is trivial. By Theorem 4.1, the parasemifield S is additively idempotent. □

We have proved in this way Theorem 1.2 (a). As we explained in the introduction, the results of [19, 21] then imply also parts (b) and (c) of the theorem.

Let us conclude by pointing out the following surprising corollary of our results.

Corollary 4.6. *Let S be a parasemifield that is finitely generated as a semiring. Then S is finitely generated as a multiplicative semigroup.*

Proof. It follows immediately from Theorems 4.5, 3.5 and Proposition 3.4. □

Acknowledgment: We wish to thank the anonymous referee for a careful reading of the manusript and for several comments and suggestions that have helped improve the article.

Funding: The first author was supported by Neuron Impulse award and by Charles University Research Centre program UNCE/SCI/022.

References

[1] L. P. Belluce and A. Di Nola, Commutative rings whose ideals form an MV-algebra, *MLQ Math. Log. Q.* **55** (2009), no. 5, 468–486.

[2] L. P. Belluce, A. Di Nola and A. R. Ferraioli, MV-semirings and their sheaf representations, *Order* **30** (2013), no. 1, 165–179.

[3] L. P. Belluce, A. Di Nola and A. R. Ferraioli, Ideals of MV-semirings and MV-algebras, in: *Tropical and Idempotent Mathematics and Applications*, Contemp. Math. 616, American Mathematical Society, Providence (2014), 59–75.

[4] W. Bruns and J. Gubeladze, *Polytopes, Rings, and K-theory*, Springer Monogr. Math., Springer, Dordrecht, 2009.

[5] M. Busaniche, L. Cabrer and D. Mundici, Confluence and combinatorics in finitely generated unital lattice-ordered abelian groups, *Forum Math.* **24** (2012), no. 2, 253–271.

[6] G. Călugăreanu and T. Y. Lam, Fine rings: A new class of simple rings, *J. Algebra Appl.* **15** (2016), no. 9, Article ID 1650173.

[7] A. Connes and C. Consani, Characteristic 1, entropy and the absolute point, in: *Noncommutative Geometry, Arithmetic, and Related Topics*, Johns Hopkins University, Baltimore (2011), 75–139.

[8] A. Connes and C. Consani, Geometry of the arithmetic site, *Adv. Math.* **291** (2016), 274–329.

[9] A. Di Nola and B. Gerla, Algebras of Lukasiewicz's logic and their semiring reducts, in: *Idempotent Mathematics and Mathematical Physics*, Contemp. Math. 377, American Mathematical Society, Providence (2005), 131–144.

[10] A. Di Nola and C. Russo, The semiring-theoretic approach to MV-algebras: A survey, *Fuzzy Sets and Systems* **281** (2015), 134–154.

[11] M. Droste, W. Kuich and H. Vogler, *Handbook of Weighted Automata*, Monogr. Theoret. Comput. Sci. EATCS Ser., Springer, Berlin, 2009.

[12] R. El Bashir, J. Hurt, A. Jančařík and T. Kepka, Simple commutative semirings, *J. Algebra* **236** (2001), no. 1, 277–306.

[13] A. Gathmann, Tropical algebraic geometry, *Jahresber. Deutsch. Math.-Verein.* **108** (2006), no. 1, 3–32.

[14] J. S. Golan, *Semirings and Their Applications*, Kluwer Academic, Dordrecht, 1999.

[15] S. N. Il'in, Y. Katsov and T. G. Nam, Toward homological structure theory of semimodules: On semirings all of whose cyclic semimodules are projective, *J. Algebra* **476** (2017), 238–266.

[16] I. Itenberg, G. Mikhalkin and E. Shustin, *Tropical Algebraic Geometry*, 2nd ed., Oberwolfach Semin. 35, Birkhäuser, Basel, 2009.

[17] Z. Izhakian and L. Rowen, Congruences and coordinate semirings of tropical varieties, *Bull. Sci. Math.* **140** (2016), no. 3, 231–259.

[18] J. Ježek, V. Kala and T. Kepka, Finitely generated algebraic structures with various divisibility conditions, *Forum Math.* **24** (2012), no. 2, 379–397.

[19] J. Ježek and T. Kepka, Finitely generated commutative division semirings, *Acta Univ. Carolin. Math. Phys.* **51** (2010), no. 1, 3–27.

[20] V. Kala, Lattice-ordered abelian groups finitely generated as semirings, *J. Commut. Algebra* **9** (2017), no. 3, 387–412.

[21] V. Kala and T. Kepka, A note on finitely generated ideal-simple commutative semirings, *Comment. Math. Univ. Carolin.* **49** (2008), no. 1, 1–9.

[22] V. Kala, T. Kepka and M. Korbelář, Notes on commutative parasemifields, *Comment. Math. Univ. Carolin.* **50** (2009), no. 4, 521–533.

[23] Y. Katsov, T. G. Nam and J. Zumbrägel, On simpleness of semirings and complete semirings, *J. Algebra Appl.* **13** (2014), no. 6, Article ID 1450015.

[24] B. Keller, Cluster algebras and derived categories, in: *Derived Categories in Algebraic Geometry*, EMS Ser. Congr. Rep., European Mathematical Society, Zürich (2012), 123–183.

[25] T. Kepka and M. Korbelář, Conjectures on additively divisible commutative semirings, *Math. Slovaca* **66** (2016), no. 5, 1059–1064.

[26] E. Leichtnam, A classification of the commutative Banach perfect semi-fields of characteristic 1: Applications, *Math. Ann.* **369** (2017), no. 1–2, 653–703.

[27] G. L. Litvinov, The Maslov dequantization, idempotent and tropical mathematics: A very brief introduction, in: *Idempotent Mathematics and Mathematical Physics*, Contemp. Math. 377, American Mathematical Society, Providence (2005), 1–17.

[28] G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, *Adv. Math. Commun.* **1** (2007), no. 4, 489–507.

[29] C. J. Monico, *Semirings and Semigroup Actions in Public-key Cryptography*, ProQuest LLC, Ann Arbor, 2002, Thesis (Ph.D.)–University of Notre Dame.

[30] D. Mundici, Interpretation of AF C^*-algebras in łukasiewicz sentential calculus, *J. Funct. Anal.* **65** (1986), no. 1, 15–63.

[31] D. Mundici, Introducing MV-algebras, preprint, http://msekce.karlin.mff.cuni.cz/~ssaos/handout_mundici.pdf.

[32] R. T. Rockafellar, *Convex Analysis*, Princeton Landmarks in Math., Princeton University Press, Princeton, 1997.

[33] F. M. Schneider and J. Zumbrägel, Every simple compact semiring is finite, *Topology Appl.* **206** (2016), 305–310.

[34] K. Thas, *Absolute Arithmetic and* $\mathbb{F}_1$*-geometry*, European Mathematical Society, Zürich, 2016.

[35] E. M. Vechtomov and A. V. Cheraneva, Semifields and their properties (in Russian), *Fundam. Prikl. Mat.* **14** (2008), no. 5, 3–54; translated in *J. Math. Sci. (N. Y.)* **163** (2009), no. 6, 625–661.

[36] H. J. Weinert, Über Halbringe und Halbkörper. I, *Acta Math. Acad. Sci. Hungar.* **13** (1962), no. 3–4, 365–378.

[37] H. J. Weinert and R. Wiegandt, On the structure of semifields and lattice-ordered groups, *Period. Math. Hungar.* **32** (1996), no. 1–2, 129–147.

[38] J. Zumbrägel, *Public-key cryptography based on simple semirings*, PhD Thesis, Universität Zürich, Zürich, 2008.

Semigroup Forum (2020) 101:406–420
https://doi.org/10.1007/s00233-020-10101-w

RESEARCH ARTICLE

Simple semirings with a bi-absorbing element

Tomáš Kepka[1] · Miroslav Korbelář[2] · Petr Němec[3]

Received: 11 August 2019 / Accepted: 16 March 2020 / Published online: 13 May 2020

Abstract

We study additively idempotent congruence-simple semirings with a bi-absorbing element. We characterize a subclass of these semirings in terms of semimodules of a special type (o-characteristic semimodules). We show that o-characteristic semimodules are uniquely determined. We also generalize a result by Ježek and Kepka on simple semirings of endomorphisms of semilattices.

Keywords Simple semiring · Bi-absorbing · Semimodule · Idempotent · Semilattice

Simple semirings are the structural keystones of semirings. A complete classification of commutative simple semirings was obtained in [1]. Finite simple semirings were classified in [6] with the exception of the case of additively idempotent semirings with a bi-absorbing element.

In this paper we provide results on additively idempotent semirings with a bi-absorbing element that will generalize the finite types studied in [6]. Our results will include also infinite cases. We give a characterization of a subclass of these semirings in terms of o-characteristic semimodules. Our main result (Theorem 2.2)

Communicated by Laszlo Marki.

The second author was supported by the project CAAS CZ.02.1.01/0.0/0.0/16_019/0000778.

✉ Miroslav Korbelář
miroslav.korbelar@gmail.com

Tomáš Kepka
kepka@karlin.mff.cuni.cz

Petr Němec
nemec@tf.czu.cz

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

[2] Department of Mathematics, Faculty of Electrical Engineering, Czech Technical University in Prague, Technická 2, 166 27 Prague 6, Czech Republic

[3] Department of Mathematics, Czech University of Life Sciences in Prague, Kamýcká 129, 165 21 Suchdol, Prague 6, Czech Republic

will be an analogy of a similar characterization achieved for the case of additively idempotent semirings with a zero [7, Theorem 5.1]. We also provide a generalization (Theorem 2.4) of a result on endomorphisms of semilattices [5, Theorem 2.2].

1 Preliminaries

A *semiring* $S = S(+, \cdot)$ is an algebraic structure equipped with two associative operations, where the addition is commutative and the multiplication distributes over the addition from both sides.

The semiring S is called (*congruence-*)*simple* if it has precisely two congruences. A (*left*) *S-semimodule* $M = {}_SM$ is a commutative semigroup $M(+)$ together with a semiring homomorphism $\varphi : S \to \mathrm{End}(M(+))$ usually denoted as an action of S on M in the form $sm := \varphi(s)(m)$ for all $s \in S$ and $m \in M$. A semimodule ${}_SM$ is called *faithful* if φ is injective (i.e., if for all $a, b \in S$, $a \neq b$, there is at least one $x \in M$ with $ax \neq bx$), *simple* if ${}_SM$ has precisely two (S-semimodule) congruences and *minimal* if $|M| \geq 2$ and for every subsemimodule ${}_SN$ of ${}_SM$ such that $|N| \geq 2$ is $N = M$. A non-empty subset I of S is a *left ideal* if $SI \cup (I + I) \subseteq I$. A left ideal I is *minimal* if it is minimal as the S-semimodule (with the natural action of S). Right semimodules and ideals are defined analogously.

The semiring S is *additively idempotent* iff $a + a = a$ for every $a \in S$. A subset K of S is called *multiplicatively idempotent* iff $a^2 = a$ for every $a \in K$.

In an (additive) semigroup $A = A(+)$, the notation $0_A \in A$ will mean that A possesses a (unique) *left and right neutral* element 0_A. Similarly, $o_A \in A$ will mean that A possesses a (unique) *left and right absorbing* element o_A. The notation $0_A \notin A$ ($o_A \notin A$, resp.) then denotes the fact that $A(+)$ has no such element.

If the semigroup A is idempotent (i.e., if it is a semilattice) we will always consider the natural ordering $a \leq b$ defined as $a + b = b$ for $a, b \in A$. In this case, $0_A \in A$ is the least and $o_A \in A$ is the greatest element in A. A subset K of A will be called *downwards closed* if the conditions $a \in K$, $b \in S$ and $b \leq a$ imply that $b \in K$.

2 Main results

Let $S = S(+, \cdot)$ be a simple semiring with a *bi-absorbing* element $o_S \in S$ (i.e., $o_S + x = o_S$ and $x \cdot o_S = o_S = o_S \cdot x$ for every $x \in S$). Such semirings can be divided into three types (I), (II) and (III).

To see this, let us first consider the relation σ on S defined as $(a, b) \in \sigma$ iff $2a = 2b$. It is a semiring congruence on S. Since S is simple, we have $|S| \geq 2$ and either $\sigma = S \times S$ or $\sigma = \mathrm{id}_S$. If $\sigma = S \times S$ then S is *additively nil of index* 2 (i.e., $2 \cdot S = \{o_S\}$). According to the basic classification in [2, Theorem 2.1], we obtain that

(I) either $S + S = S$ and S is infinite, by [4, Corollary 8.3] (for an example see [3])

(II) or $S + S = \{o_S\}$ and the multiplicative semigroup of S is congruence-simple (many natural examples are available).

On the other hand, let $\sigma = \mathrm{id}_S$. As $a + o_S = o_S = b + o_S$ for all $a, b \in S$, the semiring S is not additively cancellative. According to the remaining case of the basic classification in [2, Theorem 2.1], we obtain that

(III) S is additively idempotent (for natural examples, see [2, 5, 6]).

A fruitful approach of how to study simple additively idempotent semirings is to view them as semirings of endomorphisms of their idempotent semimodules (semilattices) [5, 6]. The case when such an S-semimodule M possesses many endomorphisms coming from S is of special importance. In this paper we will deal with the following notion.

Definition 2.1 Let S be a non-trivial semiring and M be an (additively) idempotent (left) S-semimodule. We shall say that M is an *o-characteristic semimodule* if the following three conditions are satisfied:

- M is faithful (and therefore $|M| \geq 2$, as S is non-trivial);
- $o_M \in M$ and $So_M = \{o_M\}$;
- There is a mapping $\varepsilon : M^* \times M \to S$, where $M^* = M \backslash \{o_M\}$, such that

$$\varepsilon(u, v)x = \begin{cases} o_M & \text{if } x \not\leq u \\ v & \text{if } x \leq u \end{cases}$$

for all $(u, v) \in M^* \times M$ and $x \in M$.

According to [6, the end of Section 6] one can prove that if a *finite* semiring S of type (III) possesses an idempotent irreducible S-semimodule M with a superfluous element (for the details, see [6]), then M is unique (up to isomorphism). It follows that such a semimodule is, in fact, o-characteristic.

In this paper we show that an o-characteristic semimodule is always unique (Theorem 3.9) and provide the following characterization (for the proof see Sect. 6).

Theorem 2.2 *Let S be an additively idempotent semiring with a bi-absorbing element o_S and $|S| \geq 3$. Assume further that $0_S \in S$ and $o_K \in K$ whenever K is a downwards closed subsemilattice of $S(+)$ such that both the sets K and $S\backslash K$ are infinite. Then the following three conditions are equivalent:*

(i) *The semiring S is simple and has at least one minimal left ideal.*
(ii) *There is an o-characteristic semimodule M.*
(iii) *S is simple and there is a faithful minimal semimodule L.*

Moreover, if these equivalent conditions are satisfied then:

(a) *Every (left) o-characteristic semimodule M is isomorphic to the multiplicatively idempotent minimal left ideal $I = S \cdot 0_S$ of S. In particular, an o-characteristic semimodule M is unique up to isomorphism.*

(b) *Every minimal left ideal of S is o-characteristic. All these minimal left ideals are isomorphic as left S-semimodules.*

Theorem 2.2 is analogous to Theorem 5.1 in [7] (see below), where the central object was an additively idempotent semiring S' *with a zero* $0_{S'} \in S'$ (i.e., $0_{S'} + x = x$ and $x \cdot 0_{S'} = 0_{S'} = 0_{S'} \cdot x$ for every $x \in S'$). The zero element $0_{S'}$ is the least element in S'. This case is essentially different from the one with a bi-absorbing element (that is, on the contrary, the greatest element) and we cannot transform one into the other by simply turning the semiring "upside-down".

Theorem 2.3 ([7], Theorem 5.1) *Let S' be an additively idempotent semiring with a zero $0_{S'}$ and $|S'| \geq 3$. Assume further that $o_{S'} \in S'$ and $o_K \in K$ whenever K is a downwards closed left ideal of S' such that both the sets K and $S' \backslash K$ are infinite. Then the following three conditions are equivalent:*

(i) *The semiring S' is simple and has at least one minimal left ideal.*

(ii) *There is a* 0*-characteristic semimodule M.*

(iii) *S' is simple and there is a faithful minimal semimodule L.*

Moreover, if these equivalent conditions are satisfied then:

(a) *Every* 0*-characteristic semimodule M is isomorphic to some minimal left ideal I of S'.*

(b) *If J is a minimal left ideal of S' then the factor-semimodule $J/\tilde{\mu}_J$ is* 0*-characteristic.*

Let us point out that also the notions used in Theorems 2.2 and 2.3 are different. According to definitions in [7], a left S'-semimodule M' is 0-*characteristic* iff M' is faithful, $0_{M'} \in M'$, $S' 0_{M'} = \{0_{M'}\}$ and there is a mapping $\tilde{\varepsilon} : M' \times M' \to S'$ such that

$$\tilde{\varepsilon}(u, v)x = \begin{cases} v & \text{if } x \nleq u \\ 0_{M'} & \text{if } x \leq u \end{cases}$$

for all $(u, v) \in M' \times M'$ and $x \in M'$. The relation $\tilde{\mu}_{N'}$ on an S'-semimodule N' with $0_{N'} \in N'$ is defined as $(x, y) \in \tilde{\mu}_{N'} \iff \{a \in S' \mid ax = 0_{N'}\} = \{a \in S' \mid ay = 0_{N'}\}$.

Finally, let us mention yet another link. For a semilattice $M(+)$ with $o_M \in M$, let us denote by $End_1(M)$ the semiring of all endomorphisms of M that preserve o_M. Every downwards closed proper subsemilattice I of $M(+)$ and every $v \in M$ provide a homomorphism $e_{I,v} \in End_1(M)$ defined as

$$e_{I,v}(x) = \begin{cases} o_M & \text{if } x \in M \setminus I \\ v & \text{if } x \in I. \end{cases}$$

Clearly, every $\varphi \in End_1(M)$ with range of cardinality at most 2 is of this form. Now, denote by $\overline{X}_1(M)$ the set of all such endomorphisms $e_{I,v}$ and $X_1(M)$ the set of all those endomorphisms $e_{I,v}$, where $o_I \in I$ (such a map then corresponds to $\varepsilon(o_I, v)$).

In [5] the following characterization was given.

Theorem 2.4 ([5], Theorem 2.2) *Let $M(+)$ be a semilattice such that $|M| \geq 2$ and $o_M \in M$. Let S be a subsemiring of $End_1(M)$ such that $\overline{X}_1(M) \subseteq S$. Then S has a bi-absorbing element and the following conditions are equivalent:*

(a) *S is simple,*
(b) *for every $a \in S$ there is $e \in \overline{X}_1(M)$ such that $e \leq a$.*

Class of these semirings includes also cases studied in [6]. We provide a generalization of this result (see Propositions 4.2 and 4.3 in Sect. 4) that can be summarized as follows.

Theorem 2.5 *Let $M(+)$ be a semilattice such that $|M| \geq 2$ and $o_M \in M$. Let S be a subsemiring of $End_1(M)$ such that $X_1(M) \subseteq S$. Then S has a bi-absorbing element and*

(i) *the following two conditions are equivalent:*

(α) *S is simple,*
(β) *for every $a \in S$ there are $e \in X_1(M)$ and $b \in S$ such that $eb \leq a$.*

(ii) *the following two conditions are equivalent:*

(γ) *S is simple and for all $w \in M^*$ and $a \in S$ the set $\{x \in M \mid ax \leq w\}$ is upwards bounded in M^* (provided that this set is non-empty),*
(δ) *for every $a \in S$ there is $e \in X_1(M)$ such that $e \leq a$.*

3 *o*-characteristic semimodules

To simplify the reading of the paper, from now on let S *always* be a non-trivial additively idempotent semiring with a bi-absorbing element $o_S \in S$. Throughout this section, assume that S has an o-characteristic (left) S-semimodule M.

Remark 3.1 For proving (in)equalities within the semiring S, the following easy observation is useful: Let N be a faithful idempotent left S-semimodule such that $o_N \in N$ and $So_N = \{o_N\}$. Then for all $a, b \in S$ it holds that

- $a = b$ iff $ax = bx$ for every $x \in N^* = N \setminus \{o_N\}$;
- $a \leq b$ iff $ax \leq bx$ for every $x \in N^*$.

Lemma 3.2 *The following assertions hold:*

(i) $\varepsilon : M^* \times M^* \to S$ *is an injective mapping.*
(ii) $\varepsilon(u, o_M) = o_S$ *for every* $u \in M^*$ *and* $o_S M = \{o_M\}$.
(iii) *If* $|M| \geq 3$, *then* $|S| \geq 4$.
(iv) *If* $|M| = 2$, *then* $S = \{0_S, o_S\}$ *and* 0_S *is multiplicatively neutral.*

Proof (i) It follows easily from comparing images and pre-images of the corresponding endomorphisms of M.

(ii) Let $a \in S$ and $z \in M$. For $\varepsilon_u := \varepsilon(u, o_M) \in S$, where $u \in M^*$, we have, by the definition, that $\varepsilon_u z = o_M$ and therefore we obtain that $(\varepsilon_u + a)z = \varepsilon_u z + az = o_M + az = o_M = \varepsilon_u z$. By Remark 3.1, it follows that $\varepsilon_u + a = \varepsilon_u$ for every $a \in S$. Thus $\varepsilon_u = o_S$. The rest is easy.

(iii) It follows from the injectivity of $\varepsilon(\cdot, \cdot)$ in (i).

(iv) By the assumption, we have that $M = \{0_M, o_M\}$ and $0_M \neq o_M$. The semigroup $\mathrm{End}(M(+))$ then consists of id_M and two constant mappings. By the faithfulness of M, the semiring S embeds into $\mathrm{End}(M(+))$ and because of $So_M = \{o_M\}$, we obtain that $|S| = 2$. The rest is easy. □

Lemma 3.3 *Let* $u, x \in M^*$, $v, y \in M$ *and* $a \in S$. *Then:*

(i) $\varepsilon(u, v)u = v$.
(ii) $a \cdot \varepsilon(u, v) = \varepsilon(u, av)$.
(iii) $\varepsilon(u, v) + \varepsilon(u, y) = \varepsilon(u, v + y)$.
(iv) $\varepsilon(x, v) \cdot \varepsilon(u, y) = \begin{cases} o_S & \text{if } y \not\leq x \\ \varepsilon(u, v) & \text{if } y \leq x. \end{cases}$

Proof It follows easily from Remark 3.1 and Lemma 3.2(ii). □

Proposition 3.4 *The following assertions hold:*

(i) $Sx = M$ *for every* $x \in M^*$.
(ii) *The* S*-semimodule* M *is minimal. The only* S*-subsemimodules of* M *are* $\{o_M\}$ *and* M.
(iii) *The semimodule* M *is simple.*

Proof The cases (i) and (ii) follow immediately from Lemma 3.3(i).

(iii) Let $\equiv$ be a congruence of M such that $u \equiv v$ for some $u, v \in M$, $u \neq v$. Since either $u \neq u + v$ or $v \neq u + v$, we can assume for instance that $u < u + v$. Then we have $u = u + u \equiv u + v$ and therefore we obtain that $u \equiv u + v = \varepsilon(u, u + v)u \equiv \varepsilon(u, u + v)(u + v) = o_M$. In particular, $su \equiv so_M = o_M$ for every $s \in M$. Now, by the case (i), $Su = M$ and it follows that $\equiv$ is equal to the trivial congruence $M \times M$. □

Lemma 3.5 *For any $a \in S$ the following conditions are equivalent:*

(i) $0_S \in S$ *and* $a = 0_S$.
(ii) $0_M \in M$ *and* $aM^* = \{0_M\}$.

Proof Assume condition (i). By Lemma 3.3(i), for every $(x, y) \in M^* \times M$ we have $0_S x + y = 0_S x + \varepsilon(x, y)x = \big(0_S + \varepsilon(x, y)\big)x = \varepsilon(x, y)x = y$. Hence $0_S x$ is the unique additively neutral element of M (i.e., $0_M \in M$ and $0_S x = 0_M$).

Now, assume condition (ii). Then for every $s \in S$ and $x \in M^*$ we obtain that $(a + s)x = ax + sx = 0_M + sx = sx$. Hence, by Remark 3.1, it follows that $a + s = s$ and $a = 0_S \in S$. □

Proposition 3.6 *For $u \in M^*$ put $T_u := \{\varepsilon(u, v) \mid v \in M\}$. Then:*

(i) *T_u is a minimal left ideal of the semiring S and the map $\varepsilon(u, \cdot) : M \to T_u$ is an S-semimodule isomorphism.*
(ii) *T_u is multiplicatively idempotent if and only if $u = o_{M^*} \in M^*$.*
(iii) *Let $0_S \in S$. Then $0_S \in T_u$ if and only if $u = o_{M^*} \in M^*$.*

Proof (i) Follows immediately from Lemma 3.3 and Proposition 3.4.

(ii) First, let $u \in M^*$ be an element such that $u < v$ for some $v \in M^*$. Then $\varepsilon(u, v) \cdot \varepsilon(u, v) = o_M \neq \varepsilon(u, v)$, by Lemma 3.3, and T_u is not multiplicatively idempotent.

Now, if $u = o_{M^*} \in M^*$, then for every $v \in M$ we have $\varepsilon(u, v) \cdot \varepsilon(u, v) = \varepsilon(u, v)$, by Lemma 3.3, and T_u is multiplicatively idempotent in this case.

(iii) Assume, on the other hand, that $u = o_{M^*} \in M^*$. Then, for every $y \in M^*$, it holds that $y \leq o_{M^*} = u$ and therefore we have $\varepsilon(u, 0_M)y = 0_M$. Hence $\varepsilon(u, 0_M)M^* = \{0_M\}$ and, by Lemma 3.5, we obtain that $0_S = \varepsilon(u, 0_M) \in T_u$. □

Proposition 3.7 *Let J be a minimal left ideal of S. Then:*

(i) *M and J are isomorphic left S-semimodules.*
(ii) *$a^2 = a$ or $a^2 = o_S$ for every $a \in J$.*
(iii) *$J = Ja$ for every $a \in J$ such that $a^2 = a$.*

(iv) *J is multiplicatively idempotent if and only if for every $a \in J \setminus \{o_S\}$ there is $u \in M^*$ such that $aM^* \leq u$.*

Proof Choose $a \in J \setminus \{o_S\}$. Then there is $z_0 \in M^*$ such that $az_0 \neq o_M$. Take $u \in M^*$ such that $az_0 \leq u$. Now, by Lemma 3.3, the map $\psi : M \to J$, $\psi(x) := \varepsilon(u, x)a$ is an S-semimodule homomorphism.

Since $\psi(z_0)z_0 = \varepsilon(u, z_0)az_0 = z_0 \neq o_M$, we have $\psi(z_0) \neq o_S$. Further, $\psi(o_M) = \varepsilon(u, o_M)a = o_S a = o_S$, and therefore $|\psi(M)| \geq 2$. Hence $\psi(M) = J$, as J is minimal, and ψ is injective, as M is simple (Proposition 3.4(iii)). Thus ψ is an isomorphism.

Finally, by Lemma 3.3, we have $\psi(x)\psi(x) = \varepsilon(u, x)a\varepsilon(u, x) a = \varepsilon(u, x)\varepsilon(u, ax)a = \varepsilon(u, x)a = \psi(x)$ if $ax \leq u$ and, similarly, $\psi(x)\psi(x) = o_S$ if $a \nleq u$. The rest now easily follows. □

Proposition 3.8 *The following are equivalent:*

(i) *S has a multiplicatively idempotent minimal left ideal.*
(ii) *There are $a \in S$ and $w \in M^*$ such that $aM^* \leq w$.*
(iii) *The set $I = \{a \in S \mid (\exists w \in M^*)\ aM^* = \{w\}\}$ is a unique multiplicatively idempotent minimal left ideal of S.*

Moreover, if these equivalent conditions are satisfied, then $M^* + M^* = M^*$.

Proof The implication (iii)⇒(i) is obvious and the implication (i)⇒(ii) follows from Proposition 3.7.

(ii)⇒(iii): Assume (ii). Then, obviously, $\varepsilon(w, w)a \in I$. Hence $J \neq \emptyset$ and it is easy to see that I is a multiplicatively idempotent minimal left ideal of S.

Now, let J be a multiplicatively idempotent minimal left ideal of S. By Proposition 3.7, there are $a' \in J \setminus \{o_S\}$ and $u \in M^*$ such that $a'M^* \leq u$. Then $o_S \neq \varepsilon(u, u)a' \in I \cap J$ and, as I and J are both minimal, we obtain that $I = J$. The rest is easy. □

Theorem 3.9 *The o-characteristic semimodule M is unique (up to isomorphism) and is isomorphic to any minimal left ideal of S.*

If $0_S \in S$, then $S0_S$ is a multiplicatively idempotent minimal left ideal of S (and it is isomorphic to M as a left S-semimodule).

Proof The first part follows from Propositions 3.6 and 3.7. Further, if $0_S \in S$ then, by Lemma 3.5, $0_M \in M$ and $0_S M^* = \{0_M\}$. By Proposition 3.8, there is a unique multiplicatively idempotent minimal left ideal I and, obviously, $0_S \in I$. Since $S0_S$ is a left ideal and $|S0_S| \geq 2$, we obtain that $S0_S = I$, by the minimality of I. □

4 When semirings with *o*-characteristic semimodules are simple

In this section we study simplicity of the semiring S. In this way we obtain several variations of Theorem 2.4. Throughout this section let us assume again that S has an o-characteristic (left) S-semimodule M.

Lemma 4.1 *Let $\varrho \neq \mathrm{id}_S$ be a congruence of the semiring S. Then $\big(\varepsilon(u,v), o_S\big) \in \varrho$ for every $(u,v) \in M^* \times M$.*

Proof There are $a, b \in S$ such that $a < b$ and $(a,b) \in \varrho$. By Remark 3.1, there is $w \in M^*$ such that $aw < bw$. Now, let $(u,v) \in M^* \times M$. By Lemma 3.3(ii) and (iv), we obtain that $\varepsilon(aw,v)a\varepsilon(u,w) = \varepsilon(aw,v)\varepsilon(u,aw) = \varepsilon(u,v)$ and $\varepsilon(aw,v)b\varepsilon(u,w) = \varepsilon(aw,v)\varepsilon(u,bw) = o_S$. Hence it follows that $\big(\varepsilon(u,v), o_S\big) = (\varepsilon(aw,v)a\varepsilon(u,w),\ \varepsilon(aw,v)b\varepsilon(u,w)) \in \varrho$. □

Proposition 4.2 *The semiring S is simple if and only if for every $a \in S$ there are $b \in S$ and $(u,v) \in M^* \times M$ such that $\varepsilon(u,v)b \leq a$.*

Proof Let $I = \{\varepsilon(u,v)b + c \mid b, c \in S, u \in M^*, v \in M\}$. By Lemma 3.3, the relation $(I \times I) \cup \mathrm{id}_S$ is a congruence of S that is non-identical. If S is simple, it follows that $I = S$.

Conversely, if $I = S$ and $\varrho \neq \mathrm{id}_S$ is a congruence of S, then, given $a \in S$, we have, by Lemma 4.1, that $\varepsilon(u,v)b \leq a$ and $(a, o_S) = (a + \varepsilon(u,v)b, a + o_S b) \in \varrho$. Hence, $\varrho = S \times S$ and the semiring S has to be simple. □

Proposition 4.3 *The following conditions are equivalent:*

(i) *For every $a \in S$ there are $u \in M^*$ and $v \in M$ such that $\varepsilon(u,v) \leq a$.*

(ii) *S is simple and for all $w \in M^*$ and $a \in S$ the set $A_{a,w} = \{x \in M \mid ax \leq w\}$ is upwards bounded in M^* (provided that this set is non-empty).*

Proof (i)⇒(ii): Let $a \in S$. Then, by (i), we have that $\varepsilon(u,v) \leq a$ for some $(u,v) \in M^* \times M$. Now, by Lemma 3.3, we obtain that $\varepsilon(u,v)b = \varepsilon(u,v) \leq a$ for $b = \varepsilon(u,u)$, and therefore, by Proposition 4.2, the semiring S is simple.

Further, choose $w \in M^*$ and let $x \in M$ be such that $ax \leq w$. Then $\varepsilon(u,v)x \leq ax \leq w < o_M$ and it follows that $x \leq u$. Therefore the set $A_{a,w}$ is upwards bounded by $u \in M^*$.

(ii)⇒(i): Let $a \in S \backslash \{o_S\}$. Since S is simple, we obtain, by Proposition 4.2, that $\varepsilon(w,v)b \leq a$ for some $(w,v) \in M^* \times M$ and $b \in S$. Further, $a \neq o_S$ and hence there is $z \in M^*$ such that $az \neq o_M$. Therefore, $\varepsilon(w,v)bz \leq az < o_M$ and it necessarily follows that $bz \leq w$. Thus, $A_{b,w} \neq \emptyset$ and, by assumption, there is $u \in M^*$ such that $A_{b,w} \leq u$.

Now, we show that $\varepsilon(u,v) \leq \varepsilon(w,v)b$. By Remark 3.1, it is enough to prove that $\varepsilon(u,v)x \leq \varepsilon(w,v)bx$ for every $x \in M^*$. If $x \in M^*$ is such that $bx \leq w$ then $x \leq u$ and we have $\varepsilon(u,v)x = v = \varepsilon(w,v)bx$. In the opposite case, when $bx \nleq w$, we always obtain that $\varepsilon(u,v)x \le o_M = \varepsilon(w,v)bx$.

Finally, $\varepsilon(u,v) \le \varepsilon(w,v)b \le a$ and this concludes our proof. □

Proposition 4.4 *If the semiring S is simple, then for every $a \in S$ there is $v \in M$ such that $v \le aM$. Conversely, if this is true and $o_{M^*} \in M^*$, then S is simple.*

Proof Assume that S is simple. By Proposition 4.2, for $a \in S$ there are $b \in S$ and $(u,v) \in M^* \times M$ such that $\varepsilon(u,v)b \le a$. Hence $v \le \varepsilon(u,v)bM \le aM$.

Conversely, let $o_{M^*} \in M^*$ and let for every $a \in S$ there be $v \in M$ such that $v \le aM$. Then for every $x \in M^*$ we have that $\big(\varepsilon(o_{M^*},v)+a\big)x = v + ax = ax$. Hence, by Remark 3.1, it follows that $\varepsilon(o_{M^*},v)+a = a$, i.e., $\varepsilon(o_{M^*},v) \le a$. Now, by Lemma 3.3, we obtain that $\varepsilon(o_{M^*},v)\cdot\varepsilon(o_{M^*},o_{M^*}) = \varepsilon(o_{M^*},v) \le a$. Hence, by Proposition 4.2, the semiring S is simple. □

Proposition 4.5 *If $0_S \in S$, then the semiring S is simple. Conversely, if the semiring S is simple and $aM^* = M^*$ for at least one $a \in S$, then $0_S \in S$.*

Proof First, let $0_S \in S$. By Lemma 3.5, we have $0_M \in M$ and $0_S M^* = \{0_M\}$. Therefore, it follows that $\big(\varepsilon(0_M,0_M)0_S\big)M^* = \{\varepsilon(0_M,0_M)0_M\} = \{0_M\}$. Hence $\varepsilon(0_M,0_M)0_S = 0_S$, again by Lemma 3.5. Now, by Proposition 4.2, the semiring S is simple.

Now, assume the other set of conditions in our statement. By Proposition 4.2, there are $b \in S$ and $(u,v) \in M^* \times M$ such that $\varepsilon(u,v)b \le a$. Since $aM^* = M^*$, for every $x \in M^*$ we have $v \le \varepsilon(u,v)bx \le ax < o_M$. It follows that $v \le aM^* = M^*$ and therefore $v = 0_M \in M$. Further, it must hold that $\varepsilon(u,0_M)bM^* = \{0_M\}$. Finally, by Lemma 3.5, we obtain that $\varepsilon(u,0_M)b = 0_S \in S$. □

5 When simple and minimal semimodules are *o*-characteristic

Throughout this section let N be an idempotent, simple and minimal S-semimodule such that $|N| \ge 3$, $o_N \in N$ and $So_N = \{o_N\}$. Assume, furthermore, that N has a minimal element $w \in N$ such that $w + N^* \subseteq N^*$ for $N^* = N \backslash \{o_N\}$ (this occurs, for instance, when $w = 0_N$).

Lemma 5.1 *$Sx = N$ for every $x \in N^*$.*

Proof The set $N' = \{x \in N \mid Sx = \{o_N\}\}$ is a subsemimodule of N and $o_N \in N'$. If $N' = N$, then $SN = \{o_N\}$ and therefore the set $\{x, o_N\}$ is a semimodule for every

$x \in N^*$. Since N is minimal, we get $|N| = 2$, a contradiction. Thus $N' = \{o_N\}$, as N is minimal, and we obtain that $Sx \neq \{o_N\}$ and $Sx = N$ for every $x \in N^*$. □

The following two lemmas are inspired by [6, Section 2.3] where, however, all structures are assumed to be finite. For the sake of completeness we therefore provide their proofs.

Lemma 5.2 *For all $u, y \in N$, $y \nleq u$, there is at least one $a \in S$ with $au = w$ and $ay = o_N$.*

Proof Define a relation σ on N by

$$(x_1, x_2) \in \sigma \;\Leftrightarrow\; \{ax_1, ax_2\} \neq \{w, o_N\} \text{ for every } a \in S.$$

This relation is reflexive and symmetric.

Further, we show that $(x_1, x_2) \in \sigma$ implies $(x_1 + x, x_2 + x) \in \sigma$ for every $x \in N$. Assume, on the contrary, that there are $x' \in N$ and $a \in S$ such that $ax_1 + ax' = w$ and $ax_2 + ax' = o_N$. By the minimality of w, we have $ax_1 = w = ax'$. Therefore, $ax_2 + w = o_N$ and, by the assumption on w, this implies that $ax_2 = o_N$. Hence $\{w, o_N\} = \{ax_1, ax_2\}$, a contradiction.

Now, it easily follows that the transitive closure τ of σ is a congruence of the semimodule M. By Lemma 5.1, $(x, o_N) \notin \sigma$ for every $x \in N^*$ and therefore the same holds for the relation τ. Hence $\tau \neq N \times N$ and, by the simplicity of N, it follows that $\tau = \sigma = \mathrm{id}_N$.

Finally, let $u, y \in N$ be such that $y \nleq u$. Then $u < u + y$ and $(u, u + y) \notin \mathrm{id}_N = \sigma$. Hence there is $a \in S$ such that $\{w, o_N\} = \{au, au + ay\}$ and $au \leq au + ay$. Therefore $au = w$ and $o_N = au + ay = w + ay$ and, by the assumption on w, it follows that $ay = o_N$, which concludes our proof. □

Lemma 5.3 *Let $u \in N^*$ and $K_u = \{a \in S \mid au = w\}$. Then:*

(i) *K_u is a (non-empty) downwards closed subsemilattice of $S(+)$.*

(ii) *If $o_{K_u} \in K_u$ then for every $v \in N$ there is $c \in S$ such that for every $x \in N$ there holds*

$$cx = \begin{cases} o_N & \text{if } x \nleq u \\ v & \text{if } x \leq u. \end{cases}$$

Proof (i) By Lemma 5.1, $K = K_u \neq \emptyset$. The rest is easy.

(ii) By Lemma 5.1, we have $bw = v$ for some $b \in S$. Put $c = bo_K$ and let $x \in N$.

Now, if $x \leq u$ then we have $o_K x \leq o_K u = w$ and, by the minimality of w, it follows that $o_K x = w$. Hence $cx = bo_K x = bw = v$ in this case.

On the other hand, if $x \nleq u$ then there is $a \in K$ such that $ax = o_N$, by Lemma 5.2. Since $o_K \geq a$, we obtain that $o_K x \geq ax = o_N$. Thus we have $o_K x = o_N$ and $cx = b(o_K x) = bo_N = o_N$. □

Proposition 5.4 *Assume that $o_K \in K$ whenever K is a downwards closed subsemilattice of $S(+)$ such that both the sets K and $S \backslash K$ are infinite. If the semimodule M is faithful, then it is o-characteristic.*

Proof For $u \in N^*$ the set $K_u = \{a \in S \mid au = w\}$ is a non-empty downwards closed subsemilattice of $S(+)$, by Lemma 5.3(i). In case that K_u is finite, we obviously have $o_{K_u} \in K_u$. If, on the other hand, K_u is infinite and N is faithful, then N has to be infinite as well. The equality $Su = N$ then, by Lemma 5.1, implies that $S \backslash K_u$ is infinite, too. Hence, by the assumption, we have $o_{K_u} \in K_u$.

Now, it holds that $o_{K_u} \in K_u$ for every $u \in N^*$. Therefore, by Lemma 5.3(ii), the module N is o-characteristic. □

6 When minimal semimodules are *o*-characteristic for simple semirings

In this section we prove Theorem 2.2. We will assume here, moreover, that the semiring S is *simple* and $|S| \geq 3$. Let N be an idempotent left S-semimodule such that $o_N \in N$ and $So_N = \{o_N\}$. Denote again $N^* = N \backslash \{o_N\}$ and define a relation μ_N on N as follows:

$$(x, y) \in \mu_N \iff \{z \in N \mid ax + z = o_N\} = \{z \in N \mid ay + z = o_N\} \text{ for every } a \in S.$$

Lemma 6.1 *If N is not faithful then $SN = \{o_N\}$. In particular, both the right S-semimodule S_S and the left S-semimodule ${}_SS$ are faithful.*

Proof The relation $\lambda_N = \{(a, b) \in S \times S \mid (\forall\, x \in N)\ ax = bx\}$ is a congruence of the semiring S. Since S is simple then either $\lambda_N = \mathrm{id}_S$ (and N is faithful) or $\lambda_N = S \times S$ (and $SN = \{o_N\}$).

Now, consider S as a left S-semimodule. It remains to show that $\lambda_S \neq S \times S$. Assume, on the contrary, that $\lambda_S = S \times S$. Then $ax = o_S x = o_S$ for all $a, x \in S$. Hence $S(+)$ is simple as a semilattice. But every such a semilattice has to be of cardinality 2, a contradiction. Thus the left S-semimodule S is faithful. The right case is symmetrical. □

Lemma 6.2 *$Sa \neq \{o_S\} \neq aS$ for every $a \in S \backslash \{o_S\}$.*

Proof If $a \in S$ is such that $Sa = \{o_S\}$, then $x(a + b) = o_S + xb = o_S = xa$ for all $x, b \in S$. By Lemma 6.1, the right S-semimodule S_S is faithful, and therefore $a + b = a$ for every $b \in S$ and $a = o_S$. The other case is symmetrical. □

Lemma 6.3 *If $w \in N^*$ is such that $Sw = N$, then $o_S N = \{o_N\}$. If, moreover, α is a congruence of N that is maximal with respect to $(w, o_N) \notin \alpha$, then the factor-semimodule N/α is both faithful and simple.*

Proof First, since $Sw = N$, for every $y \in N$ there is $c \in S$ such that $y = cw$. Hence $o_S w + y = o_S w + cw = (o_S + c)w = o_S w$ for every $y \in S$ and it follows that $o_S w = o_N$. As o_N is multiplicatively absorbing, we obtain that $o_S y = (o_S c)w = o_S w = o_N$ for every $y \in N$.

Further, from $Sw = N$ it follows that $|S(N/\alpha)| = |N/\alpha| \neq 1$ and, by Lemma 6.1, the semimodule N/α is faithful.

Finally, let ϱ be a congruence of N such that $\alpha \subsetneqq \varrho$. Then $(w, o_N) \in \varrho$. Since $Sw = N$ and $So_N = \{o_N\}$, we immediately have that $(x, o_N) \in \varrho$ for every $x \in N$. Hence $\varrho = N \times N$ and the semimodule N/α is therefore simple. □

Proposition 6.4 *Let $|N| \geq 2$ and $Sv = N$ for every $v \in N^*$. Then:*

(i) *μ_N is a congruence of the semimodule N and the one-element subsemimodule $\{o_N\}$ is a block of μ_N.*

(ii) *μ_N is the greatest (non-trivial) congruence of N.*

(iii) *The factor-semimodule N/μ_N is faithful, minimal and simple.*

(iv) *If $N^* + N^* = N^*$, then $(x, y) \in \mu_N$ if and only if*

$$\{a \in S \mid ax = o_N\} = \{a \in S \mid ay = o_N\}$$

for all $x, y \in N$.

Proof (i) The verification that μ_N is a congruence is easy. Now, let $x \in N$ be such that $(o_N, x) \in \mu_N$. Then $ax + z = o_N$ for all $a \in S$ and $z \in N$. Thus, in particular, $ax = ax + ax = o_N$. Hence $Sx = o_N$ and, by Lemma 6.2, it follows that $x = o_N$. So $\{o_N\}$ is a block of μ_N.

(ii) By (i), the congruence μ_N is non-trivial. Let α be a non-trivial congruence on N. Assuming that $(o_N, v) \in \alpha$ for some $v \in N^*$ we obtain, with the help of $Sv = N$ and $So_N = \{o_N\}$, that $\alpha = N \times N$, a contradiction. Therefore $\{o_N\}$ is a block of α. Now, let $(x, y) \in \alpha$ and let $a \in S$ and $z \in N$ be such that $ax + z = o_N$. Then $(ay + z, o_N) = (ay + z, ax + z) \in \alpha$ and this means that $ay + z \in \{o_N\}$. Hence $\alpha \subseteq \mu_N$.

(iii) Since N is minimal, the semimodule N/μ_N is minimal as well. The rest follows immediately from Lemma 6.3.

(iv) Denote by τ the other relation described in condition (iv) and choose $x, y \in N$ and $a \in S$. If $(x, y) \in \mu_N$ and $ax = o_N$ then we have $ax + z' = o_N$ for $z' = ay$ and, henceforth, $o_N = ay + z' = ay$ and $(x, y) \in \tau$. For the reverse implication, let $(x, y) \in \tau$ and let $z \in N^*$ be such that $ax + z = o_N$. From $N^* + N^* = N^*$ it follows that $ax = o_N$. By our assumption we have $ay = o_N$. Hence $ay + z = o_N$ and therefore $(x, y) \in \mu_N$. □

Proposition 6.5 *Let I be a minimal left ideal of S. Then:*

(i) $o_S \in I$ *and* $Sa = I$ *for every* $a \in I\backslash\{o_S\}$.
(ii) *The semimodule* ${}_SI$ *is faithful.*
(iii) μ_I *is the greatest (non-trivial) congruence of* ${}_SI$.
(iv) *The factor-semimodule* I/μ_I *is faithful, minimal and simple.*

Proof The assertion (i) follows easily from Lemma 6.2. To prove (ii), we use that $|SI| \neq 1$, by Lemma 6.2. Hence, by Lemma 6.1, the semimodule ${}_SI$ is faithful. Finally, (iii) and (iv) follow immediately from Proposition 6.4. □

Lemma 6.6 *Assume that* $0_S \in S$. *If I is a minimal left ideal of S, then* $0_I \in I$ *and* $0_Sa = 0_I$ *for every* $a \in I\backslash\{o_S\}$.

Proof Let $a \in I\backslash\{o_S\}$. We have $ba + 0_Sa = (b + 0_S)a = ba$ for every $b \in S$. By Proposition 6.5(i), we have $Sa = I$, and hence we obtain that $0_Sa \leq Sa = I$. Therefore $0_Sa = 0_I \in I$. □

We are in the position to prove the main result.

Proof of Theorem 2.2 (i)⇒(ii): Let J be a minimal left ideal. By Proposition 6.5, the factor-semimodule $\tilde{J} = J/\mu_J$ is faithful, minimal and simple. Besides, we have $0_J \in J$, by Lemma 6.6, and therefore $0_{\tilde{J}} \in \tilde{J}$. Since $|S| \geq 3$, it follows, by the faithfulness of $\tilde{J}$, that $|\tilde{J}| \geq 3$. Thus $\tilde{J}$ is o-characteristic, by Proposition 5.4.

(ii)⇒(iii): Combine Propositions 4.5 and 3.4(ii).

(iii)⇒(ii): Set $H = \{x \in L \mid |Sx| = 1\}$. Then we have $o_Sx \in H$ for every $x \in L$ and H is a subsemimodule. Since L is faithful, it follows that $H \neq L$ and, as L is minimal, there is $w \in L$ with $H = \{w\} = o_SL$.

Further, from $H \neq L$ we obtain that $|SL| > 1$ and, by the minimality of L, we have $SL = L$. Therefore, as the semiring S is additively idempotent, the semimodule $SL = L$ is idempotent as well.

Now, for all $a \in S$ and $x \in L$ we have $w + ax = o_Sx + ax = o_Sx = w$. Hence $L = SL \leq w$ and it follows that $w = o_L \in L$. From $o_So_L \in o_SL = \{o_L\}$ and $|So_L| = 1$ we immediately obtain that $So_L = \{o_L\}$.

Finally, for $x \in L^* = L\backslash\{o_L\}$ is $|Sx| > 1$ and, by minimality of L, we have that $Sx = L$. Hence, by Proposition 6.4(iii), the factor-semimodule $\tilde{L} = L/\mu_L$ is faithful, minimal and simple.

Also, from $ay = (0_S + a)y = 0_Sy + ay$ for all $a \in S$ and $y \in L$ we obtain that $0_Sv \leq Sv = L$ and $0_Sv = 0_L \in L$ for every $v \in L^*$. In particular, $0_{\tilde{L}} \in \tilde{L}$. Since $|S| \geq 3$ and $So_{\tilde{L}} = \{o_{\tilde{L}}\}$, it follows, by the faithfulness of $\tilde{L}$, that $|\tilde{L}| \geq 3$. Now, by Proposition 5.4, $\tilde{L}$ is o-characteristic.

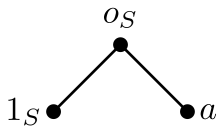
(ii)⇒(i): Combine Propositions 4.5 and 3.6(i).

Finally, the assertions (a) and (b) follow from Proposition 3.7 and Theorem 3.9.

□

Remark 6.7 There are just two (additively idempotent) two-element semirings with a bi-absorbing element (up to isomorphism). One of them possesses an o-characteristic semimodule (the one with a multiplicatively neutral element), while the other not (the one with a constant multiplication).

Example 6.8 Consider the commutative three-element semiring S with the following Hasse diagram:



Here o_S is bi-absorbing, 1_S is multiplicatively neutral and $a \cdot a = 1_S$. Clearly, S is simple, $0_S \notin S$ and no o-characteristic semimodule exists (otherwise $|S| = 2$, by Lemma 3.2(iii) and (iv)).

At the end of this paper we would like to formulate a conjecture based on Theorem 3.9 and Proposition 3.4 and related to [6, Conjecture 2.8].

Conjecture *Let S be an additively idempotent semiring with a bi-absorbing element. Then every minimal left ideal of S is simple* (*as a left S-semimodule*).

References

1. El Bashir, R., Hurt, J., Jančařík, A., Kepka, T.: Simple commutative semirings. J. Algebra **236**, 277–306 (2001)
2. El Bashir, R., Kepka, T.: Congruence-simple semirings. Semigroup Forum **75**, 588–608 (2007)
3. Flaška, V.: One very particular example of a congruence-simple semirings. Eur. J. Comb. **30**, 759–763 (2009)
4. Flaška, V., Kepka, T., Šaroch, J.: Bi-ideal-simple semirings. Comment. Math. Univ. Carolin. **46**(3), 391–307 (2005)
5. Ježek, J., Kepka, T.: The semiring of 1-preserving endomorphisms of a semilattice. Czechoslovak Math. J. **59**(134), 999–1003 (2009)
6. Kendziorra, A., Zumbrägel, J.: Finite simple additively idempotent semirings. J. Algebra **388**, 43–64 (2013)
7. Kepka, T., Kortelainen, J., Němec, P.: Simple semirings with zero. J. Algebra Appl. **15**(3), 1650047-1–1650047-9 (2016). https://doi.org/10.1142/S021949881650047X