Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DISERTAČNÍ PRÁCE

Miroslav Korbelář

Konstrukce komutativních polookruhů a radikálových okruhů

Katedra algebry
Vedoucí disertační práce: Prof. RNDr. Tomáš Kepka, DrSc.
Studijní program: Matematika
Studijní obor: Algebra, teorie čísel a matematická logika

Charles University in Prague
Faculty of Mathematics and Physics

DISSERTATION

Miroslav Korbelář

Constructions of commutative semirings and radical rings

Department of Algebra
Supervisor: Prof. RNDr. Tomáš Kepka, DrSc.
Study programme: Mathematics
Specialization: Algebra, number theory and mathematical logic

Chtěl bych velmi poděkovat své rodině a přátelům, Grantové Agentuře Univerzity Karlovy (grant 301-10/259224) a svému školiteli Prof. RNDr. Tomáši Kepkovi, DrSc., bez jejichž podpory by tento dokument nevznikl.

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

V Praze dne 30.9.2009 Miroslav Korbelář

Contents

Název práce: Konstrukce komutativních polookruhů a radikálových okruhů
Autor: Miroslav Korbelář
Katedra (ústav): Katedra algebry
Vedoucí disertační práce: Prof. RNDr. Tomáš Kepka, DrSc.
e-mail vedoucího: Tomas.Kepka@mff.cuni.cz

Abstrakt: V této disertaci se budeme zabývat konstruktivními metodami aplikovanými na komutativní polookruhy a komutativní radikálové okruhy.

V kapitole 2 budeme studovat třídu komutativních subdiretně ireducibilních radikálových okruhů. Uvedeme několik konstrukčních přístupů a pomocí reflexe z kategorie komutativních okruhů do kategorie komutativních radikálových okruhů odvodíme řadu příkladů s různými vlastnostmi. Ukážeme, že okruh $S \in \mathcal{S}$ je noetherovský právě když je konečný. Dále uvedeme částečné výsledky v klasifikaci faktorů okruhů v $\mathcal{S}$ podle monolitu.

V kapitole 3 pomocí p-prvočíselných valuací každému podpolookruhu v $\mathbb{Q}^+$ přiřadíme množinu jeho characteristických posloupností. Nalezneme a klasifikujeme všechny maximální podpolookruhy kladných racionálních čísel a ukážeme, že každý vlastní podpolookruh v $\mathbb{Q}^+$ je obsažen v nějakém z nich. Tento výsledek byl publikován v [16].

V kapitole 4 zkonstruujeme, použitím metod z kapitoly 4, novou širokou podtřídu třídy $\mathcal{C}ong\mathcal{S}imp$ všech vlastních kongruenčně jednoduchých podpolookruhů v $\mathbb{Q}^+$, klasifikujeme všechny maximální prvky v $\mathcal{C}ong\mathcal{S}imp$ a ukážeme, že každý prvek $\mathcal{C}ong\mathcal{S}imp$ je obsažen alespoň v jednom z nich.

V kapitole 5 nalezneme ekvivalentní podmínku pro to, aby polookruh $\mathbb{Q}^+[\alpha] \subseteq \mathbb{C}$, $\alpha \in \mathbb{C}$, byl obsažen v nějakém parapolotělese v $\mathbb{C}$ a provedeme klasifikaci pro případ, kdy α je algebraický prvek stupně 2. Tento výsledek je publikován v [18].

Klíčová slova: subdirektně ireducibilní, radikálový okruh, polookruh, racionální číslo, kongruenčně jednoduchý, parapolotěleso

Title: Constructions of commutative semirings and radical rings
Author: Miroslav Korbelář
Department: Department of Algebra
Supervisor: Prof. RNDr. Tomáš Kepka, DrSc.
Supervisor's e-mail address: Tomas.Kepka@mff.cuni.cz

Abstract: In this dissertation we deal with constructive methods applied to the commutative semirings and commutative radical rings.

In Chapter 2 we study the class $\mathcal{S}$ of the commutative subdirectly irreducible radical rings. We present a few constructive methods for them and using the reflection of the category of the commutative rings into the category of the commutative radical rings we derive a lot of examples of rings in $\mathcal{S}$ with various properties. We prove that a ring $S \in \mathcal{S}$ is noetherian if and only if it is finite. We show partial results in the classification of factors of $\mathcal{S}$ modulo monoliths.

In Chapter 3 we introduce, using the p-prime valuation for all primes p, a set of characteristic sequences that can be assign to every subsemiring of $\mathbb{Q}^+$. We find and classify all maximal subsemirings of positive rational numbers and show that every proper subsemiring of $\mathbb{Q}^+$ is contained in at least one of them. This results was published in [16].

In Chapter 4 we construct, using the approach from the Chapter 4, a new large subclass of the class $\mathcal{C}ong\mathcal{S}imp$ of all proper congruence-simple subsemirings of $\mathbb{Q}^+$, classify all the maximal elements of $\mathcal{C}ong\mathcal{S}imp$ and show that every element of $\mathcal{C}ong\mathcal{S}imp$ is contained in at least one of them.

In Chapter 5 we find an equivalent condition under which is the semiring $\mathbb{Q}^+[\alpha] \subseteq \mathbb{C}$, $\alpha \in \mathbb{C}$, contained in a parasemifield of $\mathbb{C}$ and make a classification for the case when α is algebraic of degree 2. This results is published in [18].

Keywords: subdirectly irreducible, radical ring, semiring, rational number, congruence-simple, parasemifield

Chapter 1

Introduction

In this dissertation we will deal with commutative semirings and commutative radical rings. The aim of this work is to study constructive methods applied to these structures and deriving examples of various properties. We will focus especially on constructions which allow a natural dealing with subsemirings of rational numbers and with subdirectly irreducible commutative radical rings. Since all structures in this thesis are considered to be commutative, we will not emphasize this fact explicitly.

Our first subject of interest - the radical rings - are ones of basic objects in commutative algebra. Especially in the case of artinian or semilocal rings (with unit), where the Jacobson radical contains a major part of the ring, they have an essential influence on the structure of such a ring. Remind also the well known fact that for an artinian ring R the factor $R/\mathcal{J}(R)$ is totally decomposable. Radical rings can be viewed from various aspects. We will mostly deal with the universal algebraic approach. Since they form a variety (with one nullary, two unary and two binary operations), the Birkhoff's theorem can be applied, and thus every radical ring is isomorphic to a subdirect product of subdirectly irreducible radical rings. Simple radical rings are just zero-multiplication rings $\mathbb{Z}_p$ for a prime p, but the subdirectly irreducible ones form a wide and colourful class of rings.

In Chapter 2 we study the class $\mathcal{S}$ of the commutative subdirectly irreducible radical rings. We present a few constructive methods for them and using the reflection of the category of the commutative rings into the category of the commutative radical rings we derive a lot of examples with various properties to investigate this class. Especially useful in this case will be the class of semiradical rings. Since this class is very close to the radical rings, many results and examples will be generalized to semiradical rings. Among other we show that:

- A ring $S \in \mathcal{S}$ is noetherian if and only if it is finite.
- There is a ring $S \in \mathcal{S}$ that is one-generated as an S-module, but not nil.
- There is a non-torsion ring $S \in \mathcal{S}$ such that $\mathrm{Ann}(S)$ is finite.
- There is a ring $S \in \mathcal{S}$ such that the torsion part of S is not reduced and $\mathrm{Ann}(S)$ is finite.
- There is a non-zero-multiplicative ring $S \in \mathcal{S}$ such that $\mathrm{Ann}(S/\mathcal{M}(S)) = 0$.

At last, we show partial results in the classification of factors of $\mathcal{S}$ modulo monoliths.

In the remaining part of the thesis we will be concerned with semirings. The notion of semirings seems to have first appeared in the literature in a 1934 paper by Vandiver [23]. Semirings are widely used in various branches of mathematics and computer science and in everyday practice as well (the semiring of natural numbers or positive rational numbers, for instance). Although this concept is a fairy basic one, they are not explored as good as the standard objects like rings and groups. The structure of subrings and subgroups of rational numbers is quite well known. On the other hand, structural properties of subsemirings and subsemigroups of $\mathbb{Q}$ are not well understood.

In Chapter 3 we introduce, using the p-prime valuation for all primes p, a set of characteristic sequences that can be assign to every subsemiring of $\mathbb{Q}^+$. Such sequences can be, on the other hand, used for construction of a semiring that is in a particular sense a good approximation of the original one. With help of this idea we find and classify all maximal subsemirings of positive rational numbers and how that every proper subsemiring of $\mathbb{Q}^+$ is contained in at least one of them. There is, surprisingly, an uncountable amount of the maximal subsemirings of $\mathbb{Q}^+$, in contrast to the countable number of maximal subrings of $\mathbb{Q}$.

In the rest of the thesis we will put our attention to the questions concerning simple-structural semirings and related problems.

Chapter 4 is a direct continuation of the previous one. Here we will look for congruence-simple semirings. They have already been characterized with the exception of the subsemirings of $\mathbb{R}^+$. Even the subsemirings of $\mathbb{Q}^+$ have not been classified yet. We construct, using the approach from the previous chapter, a new large subclass of the class $\mathcal{CongSimp}$ of all proper congruence-simple subsemirings of $\mathbb{Q}^+$, classify all the maximal elements of $\mathcal{CongSimp}$ and show that every element of $\mathcal{CongSimp}$ is contained in at least one of them. Moreover, it seems that the presented class could include all the congruence-simple subsemirings of $\mathbb{Q}^+$.

Further, it is known that every infinite finitely generated congruence-simple semiring is additively idempotent. On the other hand, it seems to be an open problem whether this remains true in the ideal-simple case. (Note that for rings these both properties coincide.) In [14] was shown that this conjecture is equivalent to the hypothesis that every parasemifield, that is finitely generated as a semiring, is additively idempotent.

By [15, 2.2], a parasemifield that is not additively idempotent contains a copy of the parasemifield $\mathbb{Q}^+$. Thus, reformulating the previous conjecture, we get a hypothesis that every (commutative) parasemifield that contains a copy of $\mathbb{Q}^+$ is not finitely generated as a semiring. (Partial results concerning that were presented in [15].) In the context of this we can naturally investigate such parasemifields that need not to be finitely generated, but are (as semirings) finitely generated over $\mathbb{Q}^+$ (i.e. there are of the form $\mathbb{Q}^+[K]$, where K is a finite set). A good starting point might be the parasemifields contained in the field of complex numbers. Although it seemed that $\mathbb{Q}^+$ was the only possible one, we find in the Chapter 5 further examples and characterize the case when the semiring $\mathbb{Q}^+[\alpha] \subseteq \mathbb{C}$ is a parasemifield, with $\alpha \in \mathbb{C}$ algebraic of degree 2 over $\mathbb{Q}$.

We will use the following usual notation: $\mathbb{N}$ ($\mathbb{N}_0$, respectively) be the set of positive (non-negative, respectively) integers; $\mathbb{Z}$ be the ring of integers; $\mathbb{Q}$ be the field of rationals; $\mathbb{R}$ be the field of reals; $\mathbb{C}$ be the field of complex numbers and $\mathbb{P}$ be the set of prime integers.

For a field $F \subseteq \mathbb{R}$ we put $F^* = F \setminus \{0\}$ and denote F^+ (F_0^+, respectively) the set of positive (non-negative, respectively) elements from F and F^- the set of negative elements from F.

Chapter 2

Commutative subdirectly irreducible radical rings

2.1 Basic facts and notions

All rings in this chapter do not need to posses a unit, also the unit does not have to be inherited by a subring and preserved by a ring homomorphism.

For a ring R we denote

$$\mathrm{Ann}(R) = \{x \in R | Rx = 0\}$$

the *annihilator of* R,

$$\mathcal{J}(R) = \bigcap \{\mathrm{Ann}_R(M) |\ M \textit{ is a simple } R\textit{-module}\}$$

the *Jacobson radical of* R,

$$\mathcal{N}(R) = \{x \in R | (\exists n \in \mathbb{N})\ x^n = 0\}$$

the *nilradical of* R,

$$\mathcal{T}(R) = \{x \in R | (\exists n \in \mathbb{N})\ nx = 0\}$$

the *torsion part of* R and

$$\mathcal{D}(R) = \sum \{D\ |D \textit{ is a divisible subgroup of } R(+)\}$$

be the *divisible part of* R.

The *Dorroh extension* of a ring R is the ring $\mathbb{D}(R) = \mathbb{Z} \oplus R$ with the multiplication given as follows: $(n,a)\cdot(m,b) = (nm, ma+nb+ab)$ for $n, m \in \mathbb{Z}$ and $a, b \in R$. We will identify R with the subring $0 \oplus R$ of $\mathbb{D}(R)$.

The set R together with the operation $a \circ b = a + b + ab$ forms an *adjoint semigroup* $R(\circ)$ of the ring R. Clearly, $R(\circ)$ is isomorphic to the multiplicative subsemigroup $1 \oplus R$ of $\mathbb{D}(R)(\cdot)$ via the map $x \mapsto 1 \oplus x$.

A ring R is *radical* if there is a ring S such that $R = \mathcal{J}(S)$ (in this case $R = \mathcal{J}(R)$).

Equivalently, a ring R is radical if and only $R(\circ)$ is a group, i.e. for every $a \in R$ there is an *adjoint element* $\widetilde{a} \in R$ such that $a + \widetilde{a} + a\widetilde{a} = 0$. This element is uniquely determined and we will use this notation for a unary operation.

Note that non-trivial radical ring R cannot contain a unit (otherwise $0 = (-1) + (\widetilde{-1}) + (-1)(\widetilde{-1}) = -1$, a contradiction).

A ring R is said to be *subdirectly irreducible* iff there exists the least non-zero ideal of R, called a *monolith* and denoted by $\mathcal{M}(R)$. Let $M \neq 0$ be an ideal of R. Clearly, a ring R is subdirectly irreducible with a monolith $\mathcal{M}(R) = M$ iff $M \subseteq Rx$ for every $x \in R \setminus \operatorname{Ann}(R)$ and $M \subseteq \mathbb{Z}x'$ for every $0 \neq x' \in \operatorname{Ann}(R)$ (i.e. iff $M \subseteq Rx + \mathbb{Z}x$ for every $0 \neq x \in R$).

We denote by $\mathcal{S}$ the class of all commutative subdirectly irreducible radical rings.

Proposition 2.1.1. [19, 12.1] *Let $R \in \mathcal{S}$. Then $\mathcal{T}(R)$ is a p-group and $\mathbb{Z}_p(+) \cong \mathcal{M}(R)(+) \subseteq \operatorname{Ann}(R)(+) \cong \mathbb{Z}_{p^n}(+)$, where $p \in \mathbb{P}$ and $1 \leq n \leq \infty$.*

For a ring R and a subset $X \subseteq R$ we say that R is *id-generated* by X iff R is generated by X as an R-module. A radical ring R is said to be *rd-generated* by $X \subseteq R$ iff R is generated by X as a radical ring.

2.2 Semiradical rings and the reflection of radical rings

An important property of the variety of the commutative radical rings is the existence of a reflection of the category of the commutative rings into the category of the commutative radical rings. We present a canonical construction of such a reflection, which will be consecutively a very effective tool for generating of examples of the class $\mathcal{S}$. As we will see, an important role in constructions of these examples will play the class of so called *semiradical* rings. We also survey when another well known construction - the semigroup algebra - is radical (semiradical, resp.).

We start with a familiar technique that uses localization.

Construction 2.2.1. Let R be a commutative ring, $\mathbb{D}(R)$ its Dorroh extension with a unit $1 = 1_{\mathbb{D}(R)}$. The set $1+R = \{(1,r) \in \mathbb{D}(R) | r \in R\}$ is a subsemigroup of the semigroup $\mathbb{D}(R)(\cdot)$. Consider the localization $(1+R)^{-1}\mathbb{D}(R)$ of $\mathbb{D}(R)$. Denote

$$\mathcal{A}(R) = (1+R)^{-1}R$$

the subring of $(1+R)^{-1}\mathbb{D}(R)$ and

$$\varphi_R : R \to \mathcal{A}(R)$$

$$r \mapsto r/1$$

the appropriate map.

Lemma 2.2.2. *Let R be a commutative ring. Then:*

(i) $\mathcal{A}(R)$ *is a radical ring,* $r/\widetilde{(1+s)} = -r/(1+r+s)$ *and* $r/(1+s) = r/1 + \widetilde{s/1} \ \cdot \ r/1$ *for every* $r, s \in R$.

(ii) $r/(1+s) = 0$ *iff* $r/1 = 0$; $\ker(\varphi_R) = \{x \in R | (\exists a \in R)\ x = ax\}$.

(iii) $\mathcal{A}(R) = 0$ *iff* $\varphi_R = 0$.

Proof. Easy. □

Now we show that $(\mathcal{A}(R), \varphi_R)$ is the desired reflection.

Proposition 2.2.3. $(\mathcal{A}(R), \varphi_R)$ *is a reflection of the category of the commutative rings into the category of the commutative radical rings (i.e. for every radical ring T and every ring homomorphism $\psi : R \to T$ there is an unique homomorphism of radical rings $f : \mathcal{A}(R) \to T$ such that $\psi = f \circ \varphi_R$).*

Proof. Due to 2.2.2, we only need to prove that the map φ_R has the appropriate properties. First, we show the uniqueness-property. Let there be a homomorphism $f : \mathcal{A}(R) \to T$ of radical rings such that $\psi = f\varphi_R$, where $\psi : R \to T$ is a given ring homomorphism. From $r/(1+s) = r/1 + r/1 \cdot \widetilde{s/1}$, by (i), follows $f(r/(1+s)) = f(r/1) + f(r/1)\widetilde{f(s/1)} = \psi(r) + \psi(r)\widetilde{\psi(s)}$ for all $r, s \in R$.

To show existence, define f as above, i.e. $f(r/(1+s)) = \psi(r)(1+\widetilde{\psi(s)})$ in the Dorroh extension $\mathbb{D}(T)$.

f is well defined: Let $r/(1+s) = r'/(1+s')$, where $r, r', s, s' \in R$, then $(1+u)w = 0$ in $\mathbb{D}(R)$ for some $u \in R$, where $w = r(1+s') - r'(1+s)$. Hence $(1+\psi(u))\psi(w) = 0$ and thus $\psi(w) = 0$, since T is a radical ring. Therefore $\psi(r)(1+\psi(s')) = \psi(r')(1+\psi(s))$ and $\psi(r)(1+\widetilde{\psi(s)}) = \psi(r)(1+\psi(s'))(1+\widetilde{\psi(s')})(1+\widetilde{\psi(s)}) = \psi(r')(1+\psi(s))(1+\widetilde{\psi(s)})(1+\widetilde{\psi(s')}) = \psi(r')(1+\widetilde{\psi(s')})$.

It is easy to show, that f is a ring homomorphism. Hence $f(\widetilde{a}) = \widetilde{f(a)}$ for every $a \in \mathcal{A}(R)$ and f is a homomorphism of radical rings. □

Lemma 2.2.4. *Let R be a commutative ring.*

(i) If R is generated by X (as a ring), then $\mathcal{A}(R)$ is rd-generated by $\varphi_R(X)$.

(ii) Let $F(X)$ be a free commutative ring with a basis X (i.e. $F(X) \cong \sum_{x\in X} x\mathbb{Z}[X]$). Then $\varphi_{F(X)}$ is injective and $\mathcal{A}(F(X))$ is a free radical ring with a basis $\varphi_{F(X)}(X)$.

(iii) Let R be a subdirectly irreducible ring. If $\varphi_R \restriction_{\mathcal{M}(R)}$ is injective, then φ_R is injective, $\mathcal{A}(R) \in \mathcal{S}$ and $\mathcal{M}(\mathcal{A}(R)) = \mathcal{M}(R)$.

(iv) Let R be id-generated by X, then $\mathcal{A}(R)$ is id-generated by $\varphi_R(X)$.

Proof. (i) Follows immediately from $r/(1+s) = r/1 + r/1 \cdot \widetilde{s/1}$ for all $s, r \in R$.

(ii) (See also [19, 11.1.2].) Let $F(X) = \sum_{x\in X} x\mathbb{Z}[X]$. Then $\varphi_{F(X)}$ is injective, by 2.2.2(ii), and $\mathcal{A}(F(X))$ is rd-generated by $\varphi_{F(X)}(X)$, by (i). Let T be a radical ring and $g : \varphi_{F(X)}(X) \to T$ a map. Then there is a ring homomorphism $\psi : F(X) \to T$ such that $g \circ (\varphi_{F(X)} \restriction_X) \subseteq \psi$. Hence there is $f : \mathcal{A}(F(X)) \to T$ a homomorphism of radical rings such that $f \circ \varphi_{F(X)} = \psi$. Thus $g \subseteq f$. Since $\varphi_{F(X)}(X)$ rd-generates $\mathcal{A}(F(X))$, is f uniquely determined.

(iii) If $\ker(\varphi_R) \neq 0$, then by assumption $\mathcal{M}(R) \subseteq \ker(\varphi_R)$ and $\varphi_R \restriction_{\mathcal{M}(R)} = 0$, a contradiction. Let $I \neq 0$ be an ideal of $\mathcal{A}(R)$. We show that $\mathcal{M}(R) \subseteq I$. Let $0 \neq r/(1+s) \in I$. Then $0 \neq r$ and thus $\mathcal{M}(R) \subseteq Rr + \mathbb{Z}r$. Since $r/1 = r/(1+s) + s/1 \cdot r/(1+s) \in I$ and φ_R is injective, we have $\mathcal{M}(R) \subseteq Rr + \mathbb{Z}r \subseteq I$. Now, from $0 \neq \mathcal{M}(R)(+) \subseteq \mathcal{M}(\mathcal{A}(R))(+) \cong \mathbb{Z}_p(+)$, by 2.1.1, follows $\mathcal{M}(R) = \mathcal{M}(\mathcal{A}(R))$.

(iv) Obvious. □

Since the reflection is constructed with help of a localization, many properties of a ring R will also be preserved in the radical ring $\mathcal{A}(R)$. In view of

2.2.4(iii), especially useful will be the case when R is embedded into $\mathcal{A}(R)$, i.e. when φ_R is injective. This brings us naturally to the following notion (see 2.2.2(ii)):

Definition 2.2.5. A commutative ring R will be called *semiradical* if and only if $(\forall x, a \in R)$ $(x = xa \Rightarrow x = 0)$.

Semiradical rings (generally non-commutative) were introduced by V. A. Andrunakievitch in [1], where also an easy equivalent description of them (in a commutative case) was presented:

Proposition 2.2.6. [1] *Let R be a commutative ring. The following are equivalent:*

(i) R is semiradical.

(ii) R is a subring of a radical ring.

(iii) The adjoint semigroup $R(\circ)$ is cancellative.

From this characterization we see that the class of semiradical rings is closed under subrings and products, contains every radical ring and, by 2.2.7(ii), also every free commutative ring. Since any non-trivial ring with unit can not be semiradical, this class is not closed under homomorphic images and thus it is not a universal algebraic variety.

In spite of this fact there also exists a reflection of the category of the commutative rings into the category of the commutative semiradical rings and it is easy to see that for a commutative ring R is this reflection of the form $(R/\ker(\varphi_R), \pi_R)$, where $\pi_R : R \to R/\ker(\varphi_R)$ is the natural projection.

Besides this reflection, there are some basic ways how to obtain semiradical rings:

Remark 2.2.7. (i) Let R be a commutative ring, then $xR[x]$ and $xR[[x]]$ are semiradical.

Indeed, for $0 \neq f = \sum_i a_i x^i \in xR[[x]]$ put $m(f) = \min\{n | a_n \neq 0\} \geq 1$. If $0 \neq f = fg$ for some $f, g \in xR[[x]]$ then $m(f) = m(fg) \geq m(f) + m(g)$. Hence $0 \geq m(g)$, a contradiction.

(ii) Let T be a domain with unit 1_T and R be a subring such that $1_T \notin R$. Then R is semiradical.

Let $a = ax$, where $a, x \in R$. Then $(1_T - x)a = 0$. Since T is a domain and $1_T \notin R$, we get $a = 0$.

We can now state basic properties of subdirectly irreducible semiradical rings:

Proposition 2.2.8. *Let R be a semiradical ring. Then:*

(i) $\mathrm{Ann}\big(\mathcal{A}(R)\big) = \mathrm{Ann}(R)$*,* $\mathcal{N}\big(\mathcal{A}(R)\big) = (1+R)^{-1}\mathcal{N}(R)$ *and* $\mathcal{T}\big(\mathcal{A}(R)\big) = (1+R)^{-1}\mathcal{T}(R)$*.*

(ii) Let R be subdirectly irreducible. Then $\mathcal{T}(R)$ is a p-group and $\mathbb{Z}_p(+) \cong \mathcal{M}(R)(+) \subseteq \mathrm{Ann}(R)(+) \cong \mathbb{Z}_{p^n}(+)$*, where $p \in \mathbb{P}$ and $1 \leq n \leq \infty$.*

Proof. (i) Let $r/(1+s) \in \mathrm{Ann}\big(\mathcal{A}(R)\big)$. Then $ru/(1+s) = 0$ for every $u \in R$. Hence $ru/1 = 0$, by 2.2.2(ii), and $ru = 0$, since R is semiradical. Thus $r \in \mathrm{Ann}(R)$ and $r/(1+s) = r/1$. The rest is similar.

(ii) Follows from (i) and 2.1.1. □

Reflection also always allows to define a covariant functor in the following way:

Let $f : R \to T$ be a ring homomorphism, $\varphi_R : R \to \mathcal{A}(R)$ and $\varphi_T : T \to \mathcal{A}(T)$ reflections. Then there is a unique homomorphism of radical rings $f^* : \mathcal{A}(R) \to \mathcal{A}(T)$ such that $f^*\varphi_R = \varphi_T f$. Hence

$$R \mapsto \mathcal{A}(R)$$

$$f \mapsto f^*$$

is a well defined covariant functor from the category of the commutative rings into the category of the commutative radical rings.

Basic properties are listed in following remark.

Remark 2.2.9. (i) If $f : R \to T$ is surjective, then f^* is surjective.

(ii) Let R be a ring with a unit, such that $\mathcal{J}(R) \neq 0$. Then the inclusion $i : \mathcal{J}(R) \to R$ is injective, but $i^* : \mathcal{J}(R) \to \mathcal{A}(R) = 0$ is a zero homomorphism.

On the other hand, if R is a semiradical ring and $\nu : T \to R$ is an injective ring homomorphism, then ν^* is, of course, injective.

(iii) The sequence of semiradical rings $0 \to 2x\mathbb{Z}[x] \xrightarrow{i} x\mathbb{Z}[x] \xrightarrow{\pi} x\mathbb{Z}_2[x] \to 0$, where i is inclusion and π natural projection, is exact, but $Im(i^*) \neq \ker(\pi^*)$. Thus the functor $\mathcal{A}$ is right exact, but not exact, even for the semiradical rings.

Indeed, denote $R = x\mathbb{Z}[x]$ and $I = 2R$. Then $Im(i^*) = \{r/(1+s) | r, s \in I\}$ and $\ker(\pi^*) = \{r/(1+s) | r \in I, s \in R\}$. We show that $2x/(1+x) \in \ker(\pi^*) \setminus Im(i^*)$. Suppose, on contrary, that $2x/(1+x) = 2xf(x)/(1+2xg(x))$ for some

$f(x), g(x) \in \mathbb{Z}[x]$. Then $2x(1+2xg(x)) = 2xf(x)(1+x)$, since R is semiradical, and thus $1+2xg(x) = f(x)(1+x)$. Using a natural projection $\sigma : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$ we obtain $1 = f(x)(1+x)$ in $\mathbb{Z}_2[x]$, a contradiction, by comparing the degrees of the polynomials.

To illustrate the fact that semiradical rings will be more useful for constructing suitable examples of the class $\mathcal{S}$ than just working with radical rings we will consider one of the natural constructions of rings - the semigroup algebra (contracted version, resp.). Remind that the *contracted semigroup algebra* $R_0[A]$ over a ring R and a semigroup A with an zero element o (i.e. $ao = o$ for all $a \in A$) is defined as $R_0[A] = R[A]/Ro$, where $R[A]$ is the usual semigroup algebra.

Following statement (see 2.2.10) shows that the contracted semigroup algebra constructed using common rings (e.g., with unit) is radical only if it is nil. Such algebras provide thus only a limited class of examples to choose. Since commutative subdirectly irreducible radical rings arise as certain factors of commutative radical rings, and we will look especially for the non-nil ones, we will need to use another constructions or use a wider class of rings.

Proposition 2.2.10. *Let R be a ring that is not radical, A be a semigroup with a zero element o and $R_0[A]$ be the contracted semigroup algebra.*

Then $R_0[A]$ is a radical ring if and only if A is nil. In this case $R_0[A]$ is nil.

Proof. ($\Leftarrow$) S is generated by the set $\{\lambda a | \lambda \in R, a \in A\}$ of nilpotent elements and hence is it a nil ring and therefore a radical ring.

($\Rightarrow$) Since $R \neq \mathcal{J}(R)$, there is at least one ring R' with unit that is an homomorphic image of R. Then $R'_0[A]$ (as an homomorphic image) is also radical and we can therefore without loss of generality assume that R contains a unit.

Suppose now, on contrary, that some $o \neq a \in A$ is not nilpotent. Then there is $\widetilde{a} = \sum_{i=1}^{n} \lambda_i a_i \in R_0[A]$ such that $a + \widetilde{a} + a\widetilde{a} = 0$, where $n \geq 1$, $0 \neq \lambda_i \in R$, $o \neq a_i \in A$ for all $i = 1, \ldots, n$ and $a_i \neq a_j$ for all $i \neq j$. We show by induction on $k \in \mathbb{N}_0$ that:

"If $k \leq n$ then $\widetilde{a} = \sum_{i=1}^{k} (-1)^i a^i + \sum_{i=k+1}^{n} \lambda'_i a'_i$ for some $0 \neq \lambda'_i \in R$ and $o \neq a'_i \in A$ such that $a'_i \neq a'_j$ for $i \neq j$."

For $k = 0$ is it obvious. Suppose now, that the statement is true for $k \geq 0$. Then

$$0 = a + \big(\sum_{i=1}^{k}(-1)^i a^i + \sum_{i=k+1}^{n} \lambda_i' a_i'\big) + a \cdot \big(\sum_{i=1}^{k}(-1)^i a^i + \sum_{i=k+1}^{n} \lambda_i' a_i'\big) =$$

$$= \big(a + \sum_{i=1}^{k}(-1)^i a^i - \sum_{i=2}^{k+1}(-1)^i a^i\big) + \sum_{i=k+1}^{n} \lambda_i' a_i' + \sum_{i=k+1}^{n} \lambda_i' a a_i' =$$

$$= (-1)^k a^{k+1} + \sum_{i=k+1}^{n} \lambda_i' a_i' + \sum_{i=k+1}^{n} \lambda_i' a a_i'.$$

Let $k < n$. If $a^{k+1} \neq a_i'$ for all $k+1 \leq i \leq n$, then, since $a^{k+1} \neq 0$, there would be $n-k+1$ pairwise different non-zero elements $a^{k+1}, a'_{k+1}, \ldots, a'_n$ and no more than $n-k$ pairwise different non-zero elements $aa'_{k+1}, \ldots, aa'_n$, which would be in contradiction with the zero combination in the sum. Hence (without loss of generality) $a^{k+1} = a'_{k+1}$.

Suppose now that $\lambda'_{k+1} \neq (-1)^{k+1}$. Then $0 = \mu a'_{k+1} + \sum\limits_{i=k+2}^{n} \lambda_i' a_i' + \sum\limits_{i=k+1}^{n} \lambda_i' a a_i'$, where $\mu = \lambda'_{k+1} + (-1)^k \neq 0$. Considering again the numbers of pairwise different non-zero elements in the sum, we get $a_i' = aa'_{\pi(i)}$ for all i and some permutation π on the set $\{k+1, \ldots, n\}$. Obviously, $a_i' = a^m a'_{\pi^m(i)}$ for all $m \in \mathbb{N}$ and $\pi^{m_0} = id$ for some $m_0 \in \mathbb{N}$. Hence $o \neq a'_{k+1} = a^{m_0} \cdot a'_{k+1}$, a contradiction, supposing $R_0[A]$ being radical. Thus $a'_{k+1} = a^{k+1}$ and $\lambda'_{k+1} = (-1)^{k+1}$.

From $\widetilde{a} = \sum\limits_{i=1}^{n}(-1)^i a^i$ and $a + \widetilde{a} + a\widetilde{a} = 0$ now follows $0 = (-1)^n a^{n+1}$ and a is nilpotent, a contradiction. □

Comparing to the radical rings, the contracted semigroup algebra is semiradical (for a ring with unit) if and only if the appropriate semigroup is also semiradical (see 2.2.13). Such semigroups thus extend a much wider class of rings, which will be very useful for the constructions in the next section.

Definition 2.2.11. Let A be a commutative semigroup. We call A *semiradical* if every $x \in A$, such that $x = ax$ for some $a \in A$, is a zero element.

Remark 2.2.12. Let K be a finite non-empty set and $\varphi : K \to K$ a map. Then there are $a \in K$ and $k \in \mathbb{N}$ such that $\varphi^k(a) = a$.

Indeed, choose $x \in K$. Since K is finite, there must be $m, n \in \mathbb{N}$, $m < n$ such that $\varphi^m(x) = \varphi^n(x)$. Now, put $a = \varphi^m(x)$ and $k = n - m$.

Proposition 2.2.13. *Let R be a ring, A be a semigroup with a zero element o and $R_0[A]$ be the contracted semigroup algebra. Then:*

(i) Let R have a non-zero idempotent. If $R_0[A]$ is semiradical, then A is semiradical.

(ii) Let A be semiradical. Then $R_0[A]$ is semiradical.

Proof. (i) Easy.

(ii) Suppose, for contradiction, that $(\sum\limits_{i=1}^{n}\lambda_i a_i)\cdot(\sum\limits_{j=1}^{m}\mu_j b_j) = \sum\limits_{i=1}^{n}\lambda_i a_i$ in $R_0[A]$, where $n, m \geq \mathbb{N}$, $\lambda_i, \mu_j \in R \setminus \{0\}$, $a_i, b_j \in A \setminus \{o\}$ for all i, j and $a_i \neq a_j$, $b_i \neq b_j$ for all $i \neq j$. From the multiplication in $R_0[A]$ follows that there are maps $\varphi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ and $\psi : \{1, \ldots, n\} \to \{1, \ldots, m\}$ such that $a_i = a_{\varphi(i)}b_{\psi(i)}$ for every $i = 1, \ldots, n$. By 2.2.12, there are $i_0 \in \{1, \ldots, n\}$ and $k \in \mathbb{N}$ such that $\varphi^k(i_0) = i_0$. Hence $a_{i_0} = a_{\varphi(i_0)}b_{\psi(i_0)} = a_{\varphi^2(i_0)}b_{\psi\varphi(i_0)}b_{\psi(i_0)} = \cdots = a_{\varphi^k(i_0)}b_{\psi\varphi^k(i_0)}b_{\psi\varphi^{k-1}(i_0)} \ldots b_{\psi(i_0)}$. Thus $o \neq a_{i_0} = a_{i_0}.b$ for some $b \in A$, a contradiction. □

Note that, unlike the contracted version, the usual semigroup algebra yields, surprisingly, different results:

Corollary 2.2.14. *Let R be a ring, A be a semigroup and $R[A]$ be the semigroup algebra. Then:*

(i) Let R be a non-radical ring. Then the semigroup algebra $R[A]$ is never a radical ring.

(ii) Let R have a non-zero idempotent and A have an idempotent (e.g., an zero element). Then $R[A]$ is not semiradical.

(iii) Let A be semiradical without a zero element. Then $R[A]$ is semiradical.

Proof. (i) Suppose that $R[A]$ is radical. Put $A' = A \cup \{o\}$, where o is a new element such that $ao = oa = oo = o$ for all $a \in A$. Then A' is a semigroup with a zero element o. Obviously $R[A] \cong R_0[A']$. Hence $R_0[A']$ is a radical ring and, by the previous lemma, must A' be nilpotent. Thus for every $a \in A$ there is $n \in \mathbb{N}$ such that $a^n = o$, a contradiction, since $o \notin A$.

(ii) Let $0 \neq e \in R$ and $a \in A$ be idempotents. Then $0 \neq eo = (eo)(eo)$. Hence $R[A]$ is not semiradical.

(iii) Again, put $A' = A \cup \{o\}$, where o is new element and set $ao = oa = oo = o$ for every $a \in A$. Then A' is a semiradical semigroup with a zero element o. Then, by 2.2.13(ii), $R_0[A']$ is a semiradical ring. Since $R[A] \cong R_0[A']$, it follows that $R[A]$ is also semiradical. □

2.3 Noetherian and artinian case

Commutative subdirectly irreducible rings were already studied by N.H. McCoy [20] and N. Divinsky [4]. In [20] was shown that these rings are of the following three types:

(α) Fields.

(β) Every element is a zero divisor.

(γ) There exists both non-divisors of zero and nilpotent elements.

The subdirectly irreducible commutative (semi)radical rings are of type (β), since the annihilator of such a ring contains the monolith and thus is nonempty (see 2.2.8(ii)). In addition, by [5, Theorem 14], if the rings of type (β) satisfy either the descending or the ascending chain condition, they are nilpotent.

We show that the only noetherian commutative subdirectly irreducible semiradical rings are the finite ones. First, we remind some basic properties.

Lemma 2.3.1. *Let R be a ring, $X \subseteq R$ be a subset. Let $X^n = 0$ for some $n \in \mathbb{N}$ and suppose that R is id-generated by X.*

Then R is generated by X as a ring and $R^n = 0$ (i.e. R is nilpotent).

Proof. Obviously, $R = X^1 + R \cdot X^1$, where $X^1 = \{\sum_i x_i | x_i \in X\}$. Now, by induction, if $R = X^1 + \cdots + X^k + R \cdot X^k$, then $R = X^1 + \cdots + X^k + (X^1 + R \cdot X^1) \cdot X^k = X^1 + \cdots + X^k + X^{k+1} + R \cdot X^{k+1}$. Hence $R = X^1 + \cdots + X^n$ and $R^n = 0$. □

Lemma 2.3.2. *Let R be a noetherian ring. Then there is $m \in \mathbb{N}$ such that $m\mathcal{T}(R) = 0$.*

Proof. Let $\mathbb{P} = \{p_1, p_2, \ldots\}$ be the set of all prime numbers. Put $I_n = \{a \in R | (\exists k \in \mathbb{N})(p_1 \ldots p_n)^k a = 0\}$. Then $\{I_n\}_{n \in \mathbb{N}}$ is an increasing sequence of ideals of R and $\mathcal{T}(R) = \bigcup_n I_n$. Hence $\mathcal{T}(R) = I_{n_0}$ for some n_0. Further, put $J_k = \{a \in R | (p_1 \dots p_{n_0})^k a = 0\}$. Then $\{J_k\}_{k \in \mathbb{N}}$ is an increasing sequence of ideals of R and $\mathcal{T}(R) = \bigcup_k J_k$. Hence $\mathcal{T}(R) = J_{k_0}$ for some k_0. Thus $(p_1 \dots p_{n_0})^{k_0} \mathcal{T}(R) = 0$. □

Lemma 2.3.3. *Let $S \in \mathcal{S}$ and $\mathcal{M}(S)$ be a p-group.*

(i) If $\mathcal{T}(S) \neq S$, then for every $n \in \mathbb{N}$ there exists a subgroup $G_n \subseteq S(+)$ such that $M \subseteq G_n \cong \mathbb{Z}_{p^n}(+)$.

(ii) A noetherian S is torsion.

Proof. (i) Let $a \in S$ be a torsion-free element, $n \in \mathbb{N}$. Then $p^{n-1}a$ is also torsion-free and hence $p^{n-1}a \notin \operatorname{Ann}(S)$, by 2.1.1. Thus there is $b \in S$ such that $0 \neq b \cdot (p^{n-1}a) \in \mathcal{M}(S)$. Therefore ba is of order p^n and we put $G_n = \langle ba \rangle$.

(ii) $\mathcal{T}(S)$ is a p-group, hence there is $n \in \mathbb{N}$ such that $p^n \mathcal{T}(S) = 0$, by 2.3.2. Suppose that $S \neq \mathcal{T}(S)$. Then, by (i), for every $k \in \mathbb{N}$ there is $a \in \mathcal{T}(S)$ of order p^k, a contradiction. □

Proposition 2.3.4. *Let $S \in \mathcal{S}$. The following are equivalent:*

(i) S is finite,

(ii) S is finitely rd-generated,

(iii) S is noetherian.

Proof. (i)⇒(ii): Obvious.

(ii)⇒(iii): It is enough to prove that a free commutative radical ring U with a finite basis is noetherian. By 2.2.4(ii), there is a free commutative ring $T = \sum_{i=1}^{n} x_i \mathbb{Z}[x_1, \dots, x_n]$ and a reflection $\varphi_T : T \to (1+T)^{-1}T$ such that $U = (1+T)^{-1}T$. We prove that every ideal I in U is finitely generated as a U-module. Obviously $K = \varphi_T^{-1}(I)$ is finitely generated T-module, since T is a noetherian ring. Hence $(1+T)^{-1}\varphi_T(K) = I$ is also finitely generated $(1+T)^{-1}T$-module.

(iii)⇒(i): S is a finitely id-generated ring. By [5, Theorem 14], S is nil and hence, by 2.3.1, finitely generated as a ring. Moreover, $mR = 0$ for some $m \in \mathbb{N}$, by 2.3.2 and 2.3.3(ii). Hence S is finite. □

Corollary 2.3.5. *Let S be a commutative subdirectly irreducible semiradical ring. Then S is noetherian if and only it is finite. In particular, if S is noetherian then it is also artinian.*

Proof. ($\Leftarrow$) Easy.

($\Rightarrow$) Let S be noetherian, then $\mathcal{A}(S) = (1+S)^{-1}S$ is also noetherian (by the argument of finitely generated ideals). By 2.3.4, $\mathcal{A}(S)$ is finite and since S is embedded into $\mathcal{A}(S)$, is S finite too. □

Now we present several examples of finite rings in $\mathcal{S}$. Remind that every finite commutative radical ring has to be nilpotent (see for instance [19, 7.12]). Using the reflection, this implies that every finite semiradical ring needs to be nilpotent and hence radical.

Example 2.3.6. (i) Let $\mathbb{Z}_{p^n}$, $n \in \mathbb{N}$, be a ring with the standard multiplication mod p^n. Put $S(k,n) = p^k\mathbb{Z}_{p^n}$, $1 \leq k < n$. The ring $S(k,n)$ is an ideal of $\mathcal{J}(\mathbb{Z}_{p^n})$, hence $S(k,n) \in \mathcal{S}$. We have

$$\mathrm{Ann}(S(k,n)) = \begin{cases} S(n-k,n) & \text{, if } 2k \leq n \\ S(k,n) & \text{, if } 2k \geq n. \end{cases}$$

(ii) Rings of the form $\mathcal{R}(F, A, \mathbb{Z}_p, \pi)$ or $\mathcal{R}(\mathbb{Z}_{p^i}, A, \mathbb{Z}_{p^k}, \nu)$ (see 2.4.8), where F is a finite field, char$F = p$, $k \in \mathbb{N}$, $k \geq i \in \mathbb{N}$ and A is the nil semigroup from 2.4.7(i). These rings are in $\mathcal{S}$ by 2.4.5.

(iii) Rings arising using the "gluing" construction (see 2.4.10) from a finite family of a finite rings from $\mathcal{S}$ with isomorphic monoliths.

Every finitely generated commutative ring is noetherian. Infinite fields are easy examples of noetherian rings that are not finitely generated. Following example shows a noetherian radical ring that is not finitely rd-generated.

Example 2.3.7. Let $R = x\mathbb{Z}_n[[x]]$, where $n = 0$ or $n \geq 2$. Then:

(i) R is id-generated by x.

(ii) R is a noetherian semiradical ring.

(iii) $\mathcal{A}(R)$ is a noetherian radical ring which is not finitely (not even countably) rd-generated.

Proof. (i) Let $f(x) = \lambda_1 x + \lambda_2 x^2 + \cdots \in R$, then $-\lambda_1 x + f(x) = xg(x) \in Rx$ for some $g(x) \in R$. Hence $f(x) \in Rx + \mathbb{Z}x$.

(ii) The ring $\mathbb{Z}_n$ is noetherian, hence $\mathbb{Z}_n[[x]]$ is noetherian. An ideal I of R is also an ideal of $\mathbb{Z}_n[[x]]$. Hence R is noetherian. By 2.2.7 (i), R is semiradical.

(iii) R is uncountable. The rest follows by localization and 2.2.2. □

Remark 2.3.8. Ring $\mathbb{Z}_{p^\infty}$, $p \in \mathbb{P}$, with a trivial multiplication is an example of a ring in the class $\mathcal{S}$ that is artinian, but not noetherian.

As was mentioned above (in [5, Theorem 14]), any artinian ring from $\mathcal{S}$ needs to be nilpotent. To find an artinian ring from $\mathcal{S}$, that is nilpotent of degree $n \in \mathbb{N}$, consider following example:

Take any finite nilpotent ring $S \in \mathcal{S}$ of degree n (use for instance 2.3.6) and "glue" it (see 2.4.10) with $\mathbb{Z}_{p^\infty}$. Such a ring will be artinian and (since S will be a subring) also nilpotent of degree n.

Finally, we mention a property of artinian semiradical rings:

Proposition 2.3.9. *Let $R \neq 0$ be a commutative artinian semiradical ring. Then* $\operatorname{Ann}(R) \neq 0$*.*

Proof. Suppose, for contradiction, that $\operatorname{Ann}(R) = 0$ and let $0 \neq a \in R$. Then there is $0 \neq b \in R$ such that $0 \neq ab$. Hence there exists a sequence $a_1, a_2, \dots$ such that $0 \neq a_{n+1} \in Ra_n$ for every $n \in \mathbb{N}$. Put $I_n = Ra_n$. Then $\{I_n\}_{n \in \mathbb{N}}$ is a decreasing sequence of ideals and $a_{n+1} \in I_n \setminus I_{n+1}$, since R is semiradical. Hence R is not artinian, a contradiction. □

2.4 Constructions of subdirectly irreducible radical rings

In this section we will present several examples and constructive methods of the subdirectly irreducible radical rings to investigate structural properties of these ring and find out what type of such rings may arise. Besides we survey the relations between the nilradical, the torsion part, the divisible part and the annihilator.

Our usual approach will be to take a subdirectly irreducible *semiradical* ring R with desired properties and then construct the reflection $\mathcal{A}(R) = (1 + R)^{-1}R$ (see 2.2.2). By 2.2.4(iii), $\mathcal{A}(R) \in \mathcal{S}$ and, since it is a localization and the reflection is a monomorphism, many of the properties of R will be preserved in $\mathcal{A}(R)$.

First we collect necessary examples to get a better insight and then we draw conclusions.

According to the proof of Birkhoff's theorem, a commutative subdirectly irreducible radical ring can be obtained in the following way:

Let R be a radical ring and $0 \neq a \in R$. By Zorn's lemma there is an ideal K of R maximal with respect to the property $a \notin K$. Then $S = R/K \in \mathcal{S}$. Moreover, $\mathcal{M}(S) = (K + Ra)/K$, if $Ra \nsubseteq K$, and $\mathcal{M}(S) = (K + \mathbb{Z}a)/K$, if $Ra \subseteq K$. (It is easy to see that every element of $\mathcal{S}$ is of this form.)

Applying this method on the one-generated F-algebras inspires us to the following construction:

Definition 2.4.1. Let A be a commutative semigroup with a zero element o. Put $\mathrm{Ann}(A) = \{a \in A | (\forall\, x \in A)\ ax = o\}$ and $A^* = A \setminus \mathrm{Ann}(A)$.

Construction 2.4.2. Let A be a commutative semigroup with a zero element o and let $\mathrm{Ann}(A) = \{o, m\}$, where $m \neq o$.

Let R be a commutative ring, $G(+)$ be a commutative group and $\varphi : R(+) \to G(+)$ be a group homomorphisms.

Put $\mathcal{R}(R, A, G, \varphi) = (\bigoplus\limits_{a \in A^*} R \cdot a) \oplus G \cdot m$ and set the multiplication as follows:

$$\Big(\sum_{a\in A^*} \lambda_a \cdot a + g \cdot m\Big) \cdot \Big(\sum_{b\in A^*} \mu_b \cdot b + h \cdot m\Big) = \sum_{c\in A^*} \big(\sum_{ab=c} \lambda_a \mu_b\big) \cdot c + \varphi\big(\sum_{ab=m} \lambda_a \mu_b\big) \cdot m$$

where $\lambda_a, \mu_b \in R$ and $g, h \in G$.

It is easy to verify that $\mathcal{R}(R, A, G, \varphi)$ is a commutative ring.

The following remark confirms, that subdirectly irreducible factors of a one-generated F-algebra are indeed of the form of 2.4.2.

Remark 2.4.3. Let F be a field. It is not difficult to show that every ideal I of a one-generated F-algebra $R = xF[x]/(x^{n+1}F[x])$, $n \in \mathbb{N}$, is of the form $I = Hx^k \oplus Fx^{k+1} \oplus \cdots \oplus Fx^n$, where $1 \leq k \leq n$ and $H(+)$ is a subgroup of $F(+)$.

Now, easily follows that any subdirectly irreducible factor of R has indeed the form $\mathcal{R}(F, A, G, \pi)$, where $A = \big\langle a |\ a^{k+1} = o \big\rangle$ is a multiplicative group with zero element o, $1 \leq k \leq n$,

$$G = \begin{cases} \mathbb{Z}_p & , \text{ if } \mathrm{char} F = p > 0 \\ \mathbb{Z}_{p^\infty}, p \in \mathbb{P} & , \text{ if } \mathrm{char} F = 0 \end{cases}$$

and $\pi : F(+) \to G(+)$ is an epimorphism of groups.

Further, we add some assumptions to the construction 2.4.2 to obtain a subdirectly irreducible semiradical ring.

Remark 2.4.4. Let A be a commutative semigroup with a zero element o.

(i) If A is nil, then A is semiradical. Indeed, from $x = ax$ follows, by induction, $x = a^n x$ for every $n \in \mathbb{N}$. Since a is nilpotent, x is a zero element.

(ii) Define a new operation " $\star$ " on the set $B = (A \setminus \operatorname{Ann}(A)) \cup \{o\}$ as follows:

$$a \star b = \begin{cases} ab & , \text{ if } ab \notin \operatorname{Ann}(A) \\ o & , \text{ if } ab \in \operatorname{Ann}(A) \end{cases}$$

where $a, b \in B$. From $(a \star b) \star c \neq o$ follows $a \star (b \star c) \neq o$. Hence $\star$ is a commutative and associative operation. Clearly, is $B(\star)$ isomorphic to $A/\sim$, where $\sim$ is a congruence generated by the set $\{o\} \times \operatorname{Ann}(A)$. We will denote the semigroup $B(\star)$ as $A/\operatorname{Ann}(A)$.

(iii) If A is semiradical, then $A/\operatorname{Ann}(A)$ is also semiradical.

Lemma 2.4.5. *Suppose assumptions from the construction* 2.4.2*. If A is semiradical, then $\mathcal{R}(R, A, G, \varphi)$ is also semiradical. Moreover, if A is nil then $\mathcal{R}(R, A, G, \varphi)$ is also nil.*

Proof. Denote $S = \mathcal{R}(R, A, G, \varphi)$. Let $x = ax$ for some $x, a \in S$. Clearly, $S/Gm \cong R_0[A/\operatorname{Ann}(A)]$. Since $A/\operatorname{Ann}(A)$ is semiradical by 2.4.4(iii), we get that S/Gm is semiradical by 2.2.13(ii). Now, since $[x] = [x] \cdot [a]$ in S/Gm, we get $x \in Gm \subseteq \operatorname{Ann}(S)$. Hence $x = ax = 0$.

The rest is obvious. □

Now we show some sufficient conditions under which will the ring from 2.4.2 be subdirectly irreducible.

Remind that every subdirectly irreducible group is of the form $\mathbb{Z}_{p^n}(+)$, where $p \in \mathbb{P}$ and $1 \leq n \leq \infty$. Hence the only rings in $\mathcal{S}$ with the trivial multiplication are just these ones.

Proposition 2.4.6. *Let A be a commutative semigroup with zero element o, $\operatorname{Ann}(A) = \{o, m\}$, $m \neq o$ and such that for every $a_1, \dots, a_n \in A^*$, $n \geq 1$, there are $1 \leq i_0 \leq n$ and $b \in A$ such that $a_{i_0} b = m$ and $a_i b = o$ for $a_i \neq a_{i_0}$.*

Further, let R be a commutative ring, G be a commutative subdirectly irreducible p-group and $\varphi : R(+) \to G(+)$ be a group homomorphism such that $\varphi(R\lambda) \neq 0$ for every $0 \neq \lambda \in R$.

Then $\mathcal{R}(R, A, G, \varphi)$ is a subdirectly irreducible ring with monolith $\mathbb{Z}_p \cdot m$ and annihilator $G \cdot m$.

Proof. Denote $S = \mathcal{R}(R, A, G, \varphi)$. If $x \in S \setminus Gm$ then $x = \sum_{i=1}^{n} \lambda_i a_i + gm$, where $n \geq 1$, $g \in G$, $0 \neq \lambda_i \in R$ and $a_i \in A^*$ for every i. By assumption, there are i_0 and $b \in A$ such that $a_{i_0} b = m$ and $a_i b = 0$, if $a_i \neq a_{i_0}$. Further, there is $\mu \in R$ such that $\varphi(\mu\lambda_{i_0}) \neq 0$. Hence $0 \neq (\mu b)x \in Gm$.

Now, easily follows that $\mathrm{Ann}(S) = Gm$ and $(Sy + \mathbb{Z}y) \cap Gm \neq 0$ for every $0 \neq y \in S$. Since G is a subdirectly irreducible p-group, we get that $\mathbb{Z}_p \cdot m$ is a monolith of S. □

In the next remark we show some examples of semigroups fulfilling the condition of 2.4.6.

Remark 2.4.7. Is is easy to see that a semigroups A is semiradical and fulfils the conditions of 2.4.6 in these cases:

(i) Let $A = \langle x_1, \ldots, x_k | \; x_i^{n_i+1} = o, i = 1, \ldots, k \rangle$ be a presentation of a commutative semigroup with zero element o, where $n_i \in \mathbb{N}$ for all i. Then $\mathrm{Ann}(A) = \{o, x_1^{n_1} \cdots x_k^{n_k}\}$.

(ii) Let $X \neq \emptyset$ be a set. Let A be a presentation of a commutative semigroup with zero element o with respect to the basis $X \cup \{m\} \cup (X \times \mathbb{N})$ (a disjoint union with a new symbol m) and relations $\big(\{m\} \cup (X \times \mathbb{N})\big)^2 = o$, $X \cdot m = o$, $xy = x(y, i) = o$ and

$$x(x, i) = \begin{cases} (x, i-1) & , \text{ if } i \geq 2 \\ m & , \text{ if } i = 1 \end{cases}$$

for every $i \in \mathbb{N}$, $x, y \in X$ and $x \neq y$. Then $\mathrm{Ann}(A) = \{o, m\}$.

(iii) The semigroup constructed in 2.5.3(3).

Now we can introduce particular examples of rings constructed in 2.4.6. (Remind also that the divisible part $\mathcal{D}$ commutes with the direct sum $\oplus$.)

Example 2.4.8. Let A be a semiradical semigroup fulfilling the conditions of 2.4.6 (e.g. see 2.4.7).

(i) Let F be a field and set

$$G = \begin{cases} \mathbb{Z}_p & , \text{ if } \mathrm{char} F = p > 0 \\ \mathbb{Z}_{p^\infty}, p \in \mathbb{P} & , \text{ if } \mathrm{char} F = 0. \end{cases}$$

Let $\pi : F \to G$ be a group epimorphism.

Then $S = \mathcal{R}(F, A, G, \pi)$ is a subdirectly irreducible semiradical ring, $\mathcal{M}(S) = \mathbb{Z}_p \cdot m$, $\mathrm{Ann}(S) = G \cdot m$,

$$\mathcal{T}(S) = \begin{cases} S & , \text{ if } \mathrm{char} F > 0 \\ \mathrm{Ann}(S) \cong \mathbb{Z}_{p^\infty} & , \text{ if } \mathrm{char} F = 0. \end{cases}$$

and

$$\mathcal{D}(S) = \begin{cases} 0 & , \text{ if } \mathrm{char} F > 0 \\ S & , \text{ if } \mathrm{char} F = 0. \end{cases}$$

(ii) Let be $p \in \mathbb{P}$, $i \in \mathbb{N}$ and $i \leq k \leq \infty$. Let $\nu : \mathbb{Z}_{p^i}(+) \to \mathbb{Z}_{p^k}(+)$ be an inclusion.

Then $S = \mathcal{R}(\mathbb{Z}_{p^i}, A, \mathbb{Z}_{p^k}, \nu)$ is a subdirectly irreducible semiradical ring, $\mathcal{M}(S) = \mathbb{Z}_p \cdot m$, $\mathrm{Ann}(S) = \mathbb{Z}_{p^k} \cdot m$ and

$$\mathcal{D}(S) = \begin{cases} 0 & , \text{ if } k < \infty \\ \mathrm{Ann}(S) \cong \mathbb{Z}_{p^\infty} & , \text{ if } k = \infty. \end{cases}$$

Remark 2.4.9. It is easy to see, that every commutative ring that is torsion and additively divisible has trivial multiplication (see for instance [19, 1.14]). This means that every such a ring from $\mathcal{S}$ needs to be a subdirectly irreducible group and hence isomorphic to $\mathbb{Z}_{p^\infty}$ for some $p \in \mathbb{P}$. In particular, every additively divisible $S \in \mathcal{S}$ that is torsion is also nil.

Using examples from 2.4.8(ii) we can find a ring in $\mathcal{S}$ that is additively divisible, but not nil. Just take $\mathcal{A}(S) \in \mathcal{S}$, where $S = \mathcal{R}(\mathbb{Q}, A, \mathbb{Z}_{p^\infty}, \pi)$ (see 2.4.8(ii)) and A be the semigroup from 2.4.7(ii).

The next construction is a direction how to "glue together" rings from $\mathcal{S}$, with isomorphic monoliths, to get a new one.

Construction 2.4.10. Let $\{S_i\}_{i \in X} \subseteq \mathcal{S}$ be a family of rings with isomorphic monoliths. Let $\{\mathrm{Ann}(S_i)\}_{i \in X}$ be a naturally directed system of groups (i.e., for every $i, j \in X$ such that $|\mathrm{Ann}(S_i)| \leq |\mathrm{Ann}(S_j)|$ there is a monomorphism $\nu_{i,j} : \mathrm{Ann}(S_i) \to \mathrm{Ann}(S_j)$ with appropriate properties).

Let $S = \bigoplus_{i \in X} S_i$ be a direct sum of rings and I be an ideal of S generated by the set $\{x - \nu_{i,j}(x) | x \in \mathrm{Ann}(S_i), |\mathrm{Ann}(S_i)| \leq |\mathrm{Ann}(S_j)|, i, j \in X\}$.

Then $S/I \in \mathcal{S}$, $\mathrm{Ann}(S/I) = \varinjlim\{\mathrm{Ann}(S_j) | j \in X\} = \big(\bigoplus_{j \in X} \mathrm{Ann}(S_j)\big)/I$, $\mathcal{M}(S/I) = \varinjlim\{\mathcal{M}(S_j) | j \in X\} = \big(\mathcal{M}(S_i) + I\big)/I$ and $\mu_i : S_i \to S/I$, $\mu_i(x) = [x]$, $x \in S_i$, is a ring monomorphism for every $i \in X$.

Proof. Denote $M_i = \mathcal{M}(S_i)$. Clearly, $M = \big(\bigoplus_{j\in X} M_j + I\big)/I$ is a direct limit of $\{M_i\}_{i\in X}$ and $N = \big(\bigoplus_{j\in X} \mathrm{Ann}(S_j)\big)/I$ is a direct limit of $\{\mathrm{Ann}(S_i)\}_{i\in X}$. Hence $M = (M_i + I)/I \cong M_i \neq 0$ for every $i \in I$ and $N \cong \mathbb{Z}_{p^n}$, where $1 \leq n \leq \infty$.

Let $0 \neq a = [\sum_i x_i] \in S/I$, $x_i \in S_i$. If $x_{i_0} \in S_{i_0} \setminus \mathrm{Ann}(S_{i_0})$ for some i_0, then there is $r_{i_0} \in S_{i_0}$ such that $0 \neq r_{i_0}x_{i_0} \in M_{i_0}$, hence $0 \neq [r_{i_0}][\sum_i x_i] = [r_{i_0}x_{i_0}] \in M$. Thus $[\sum_i x_i] \notin \mathrm{Ann}(S/I)$. On the other hand, if $x_i \in \mathrm{Ann}(S_i)$ for every i, then $0 \neq a \in N \cong \mathbb{Z}_{p^n}$, hence $0 \neq p^k a \in M \subseteq N$ for some $k \in \mathbb{N}$.

Therefore M is the least nonzero ideal of S/I and $\mathrm{Ann}(S/I) = N$.

Finally, since $I \subseteq \bigoplus_{j\in X} \mathrm{Ann}(S_j)$ and $\mathrm{Ann}(S_i)$ is embedded into N, we get that $x = 0$ for every $x \in \mathrm{Ann}(S_i) \cap I$. Hence μ_i is a monomorphism for every $i \in X$. □

In the next part we will construct subdirectly irreducible rings with help of the subdirectly irreducible modules.

Remind that for a commutative ring R and a commutative R-algebra K is $R \oplus K$ with the multiplication given as $(r,x)\cdot(s,y) = (rs, ry + sx + xy)$, where $r, s \in R$, $x, y \in K$, again a commutative ring, that contains R and K as subrings. If K is only an R-module, we will suppose the multiplication on K to be trivial.

Lemma 2.4.11. *Let N be a R-module.*

(i) If R is a semiradical ring and $\mathrm{Fix}_N(r) = \{a \in N | ra = a\} = 0$ *for every $r \in R$, then $R \oplus N$ is semiradical.*

(ii) Let N be a faithful (i.e. $\mathrm{Ann}_R(N) = \{r \in R | (\forall a \in N) ra = 0\} = 0$*) subdirectly irreducible R-module with a monolith M.*
Then $S = R \oplus N$ is a subdirectly irreducible ring, $\mathcal{M}(S) = M$ and $\mathrm{Ann}(S) = \{a \in N | (\forall r \in R) ra = 0\}$.

Proof. (i) Easy.

(ii) Clearly, M is an ideal of S. Let $0 \neq x = (r,a) \in S$. We need to show that $M \cap (Sx + \mathbb{Z}x) \neq 0$. We can assume that $r = 0$ (and $a \neq 0$), since for $r \neq 0$ there is $x \in N$ such that $rx \neq 0$, thus $0 \neq (0, rx) = (r,a)(0,x) \in Sx + \mathbb{Z}x$. Now, since $a \neq 0$ and M is a subdirectly irreducible R-module, we have $0 \neq M \cap (Ra + \mathbb{Z}a) \subseteq M \cap (Sx + \mathbb{Z}x)$.

The rest is easy. □

We already know that a finitely rd-generated ring in $\mathcal{S}$ has to be finite (se 2.3.4), hence nil. Now we present an example of a ring $S \in \mathcal{S}$, that is just κ-id-generated for a given cardinal $\kappa \neq 0$, but not nil.

Example 2.4.12. Let X be a non-empty set, $k \in \mathbb{N} \cup \{\infty\}$. Let m be a new symbol, $A = \{e_i\}_{i \in (X \times \mathbb{N}) \cup \{m\}} \cup \{o\}$ be a semigroup with trivial multiplication and zero element o. Let $N = (\mathbb{Z}_{p^k})_0[A]$ be the contacted semigroup algebra. Put

$$T(X) = \begin{cases} \bigoplus_{x \in X} x\mathbb{Z}_{p^k}[x] & , \ k \in \mathbb{N} \\ \bigoplus_{x \in X} x\mathbb{Z}[x] & , \ k = \infty \end{cases}$$

a direct sum of rings.

For $x \in X$ let $\alpha_x \in End(N(+))$ be an endomorphism such that

$$\alpha_x(\lambda e_i) = \begin{cases} \lambda e_{(x,l-1)} & , \ i = (x,l) \text{ and } l \geq 2 \\ \lambda m & , \ i = (x,1) \\ 0 & , \ i = m \end{cases}$$

where $\lambda \in \mathbb{Z}_{p^k}$, $i \in (X \times \mathbb{N}) \cup \{m\}$.

Since $\alpha_x \circ \alpha_y = 0$ for $x \neq y$, there is a ring endomorphism

$$\alpha : \bigoplus_{x \in X} x\mathbb{Z}[x] \to End(N(+))$$

$$x \mapsto \alpha_x$$

for every $x \in X$. Since $p^k x\mathbb{Z}[x] \subseteq \ker(\alpha)$ for every $x \in X$ (in case $k < \infty$), N is a $T(X)$-module. Further:

(i) $R = T(X) \oplus N$ is a subdirectly irreducible semiradical ring, $\mathcal{M}(R) = \mathbb{Z}_p \cdot m$ and $\operatorname{Ann}(R) = \mathbb{Z}_{p^k} \cdot m$.

(ii) $S = \mathcal{A}(R) \in \mathcal{S}$ is id-generated by X and is not a nil ring. Moreover, if S is id-generated by a set $Y \subseteq S$, then $|Y| \geq |X|$.

(iii) $\operatorname{Ann}(S) = \mathbb{Z}_{p^k} \cdot m$,

$$\mathcal{N}(S) = \begin{cases} (1+R)^{-1}(pT(X) \oplus N) & , \ k \in \mathbb{N} \\ (1+R)^{-1}N & , \ k = \infty \end{cases}$$

and

$$\mathcal{D}(S) = \begin{cases} 0 & , \ k \in \mathbb{N} \\ (1+R)^{-1}N & , \ k = \infty. \end{cases}$$

Proof. (i) First, we show that R is semiradical. For $0 \neq a = \lambda m + \sum_i \lambda_i e_i \in N \setminus \mathbb{Z}_{p^k} \cdot m$ denote $D(a) = \min\{l \in \mathbb{N} | (\exists x \in X) \lambda_{(x,l)} \neq 0\}$, for $0 \neq a \in \mathbb{Z}_{p^k} \cdot m$ put $D(a) = 0$ and, finally, set $D(0) = -1$. Now, clearly $D(f \cdot a) < D(a)$ for every $f \in T(X)$ and $0 \neq a \in N$. Hence $\mathrm{Fix}_N(f) = 0$ for every $f \in T(X)$ and R is semiradical by 2.4.11(i).

Now, we show that N is a faithful $T(X)$-module. Let $0 \neq f = \sum_{x,n} \lambda_{(x,n)} x^n \in T(X)$ and $n_0 \in \mathbb{N}$ be the least such that $\lambda_{(x_0,n_0)} \neq 0$ for some $x_0 \in X$. Clearly, there is $\mu \in \mathbb{Z}_{p^k}$ such that $\lambda_{x_0,n_0}\mu \neq 0$. Put $a = \mu e_{(x_0,n_0)} \in N$. Then $fa \neq 0$. Hence N is a faithful $T(X)$-module.

Finally, we prove that the $T(X)$-module N is subdirectly irreducible with monolith $\mathbb{Z}_p \cdot m$. Let $0 \neq a = \lambda m + \sum_i \lambda_i e_i \in N$. If $D(a) = l \geq 1$ and $\lambda_{(x_0,l)} \neq 0$, for some $x_0 \in X$, then $0 \neq x_0^l a \in \mathbb{Z}_p \cdot m$. If $D(a) = 0$ then $0 \neq p^j a \in \mathbb{Z}_p \cdot m$, for some $j \in \mathbb{N}_0$. Hence N is a subdirectly irreducible $T(X)$-module with monolith $\mathbb{Z}_p \cdot m$.

The rest now easily follows using 2.4.11.

(ii) By 2.2.4, S is id-generated by X. Since $T(X)$ is a subring of S, is S not nil. Now, let R be id-generated by Y. Put $I = pR + N + \sum_{x \in X} xT(X)$. Then I is an ideal of R. Let $\pi : R \to R/I$ be a natural homomorphism. Since $\pi^* : \mathcal{A}(R) \to \mathcal{A}(R/I)$ is an epimorphism, is $\mathcal{A}(R/I)$ id-generated by $\pi^*(Y)$. Hence $\mathcal{A}(R/I) \cong (\mathbb{Z}_p)^{(X)}$ is generated by $\pi^*(Y)$ as a vector space over $\mathbb{Z}_p$ and thus $|X| = \dim \mathcal{A}(R/I) \leq |\pi^*(Y)| \leq |Y|$.

(iii) The annihilator follows by 2.4.11. For $k \in \mathbb{N}$ and the ring of polynomials $\mathbb{Z}_{p^k}[x]$ is $\mathcal{N}(\mathbb{Z}_{p^k}[x]) = p\mathbb{Z}_{p^k}[x]$. Further $(f+a)^n = f^n + nf^{n-1}a$ for every $f \in T(X)$, $a \in N$ and $n \in \mathbb{N}$. The rest now follows easily (use again the commutativity between the divisible part and the direct sum). □

Note that in case $k \in \mathbb{N}$ (not for $k = \infty$!) the ring R from 2.4.12 is isomorphic to $\mathcal{R}(\mathbb{Z}_{p^k}, A, \mathbb{Z}_{p^k}, \mathrm{id}_{\mathbb{Z}_{p^k}}) = (\mathbb{Z}_{p^k})_0[A]$, where A is the semigroup from 2.4.7(ii).

Now we have gathered enough examples to try to answer whether in the class $\mathcal{S}$ is possible to reverse some standard implications that hold in the class of all commutative rings (radical rings, respectively) - see the remarks 2.4.13 and 2.4.14.

Remark 2.4.13. For a ring R we have the following sequence of implications:

R is a zero-multiplication ring $\overset{(1)}{\Rightarrow}$ R is nilpotent $\overset{(2)}{\Rightarrow}$ R is a nil ring $\overset{(3)}{\Rightarrow}$ R is a radical ring.

Even in the class $\mathcal{S}$, no two of these properties coincide. Consider following counterexamples: for (1) see 2.3.6(ii), for (2) see 2.4.16 and for (3) see 2.4.12.

Remark 2.4.14. For a radical ring S and a subset $Y \subseteq S$ we have this sequence of implications:

S is generated by Y (as a ring) $\overset{(1)}{\Rightarrow}$ S is rd-generated by Y (i.e. generated as a radical ring) $\overset{(2)}{\Rightarrow}$ S is id-generated by Y (i.e. generated as an R-module).

Now we have a look at whether these implication can be reversed for $S \in \mathcal{S}$.

(i) Implication (1) can be reversed for Y finite. Indeed, by 2.3.4, every finitely rd-generated $S \in \mathcal{S}$ is finite and hence nilpotent (see for instance [19, 10.4]). Now by 2.3.1, S is generated by Y.

(ii) Implication (1) can not be generally reversed for infinite cardinality of Y. Actually, consider the ring $S = \mathcal{A}(T(X) \oplus N)$ from 2.4.12 and put $Y = X \cup \{e_i\}_{i \in (X \times \mathbb{N}) \cup \{m\}}$, where X is infinite. Then $|Y| = |X|$ and Y rd-generates S. On the other hand, take the natural projection $\pi : T(X) \oplus N \to T(X)$. If Y generates S then $\pi^*(Y) = \pi^*(X)$ generates $\pi^*(S) = \mathcal{A}(T(X)) = \oplus_{x \in X} \mathcal{A}(T(x))$. But this is impossible, since $\pi^*(x) = x/1$ does not generates a free radical ring $\mathcal{A}(T(x))$ (see 2.2.4(ii)).

(iii) Implication (2) can not be generally reversed for any (non-zero) cardinality of Y. Indeed, suppose again the ring $S = \mathcal{A}(T(X) \oplus N)$ from 2.4.12 and put $Y = X$. By 2.4.12(ii), S is generated by Y. Since $T(X) \oplus N$ is semiradical, we have, by 2.2.9(ii), that $\mathcal{A}(T(X))$ is a proper subring of S. Since Y rd-generates $\mathcal{A}(T(X))$, it does not rd-generates S. Moreover, by 2.3.4, S is not even finitely rd-generated.

It is well known that for a commutative ring S holds $\mathcal{D}(S) \cdot \mathcal{T}(S) = 0$ (see for instance [19, 1.13.(iii)]). This implies $\big(\mathcal{D}(S) \cap \mathcal{T}(S)\big)^2 = 0$ and $\mathcal{D}(S) \cap \mathcal{T}(S) \subseteq \mathcal{N}(S)$. It is natural to ask whether there are some other (non-trivial) relations (inclusions, in particular) between the ideals $\mathcal{N}(S)$, $\mathcal{T}(S)$,

$\mathcal{D}(S)$, $\mathcal{D}(S) \cap \mathcal{N}(S)$, $\mathcal{T}(S) \cap \mathcal{N}(S)$ and $\mathcal{D}(S) \cap \mathcal{T}(S)$ in the case when $S \in \mathcal{S}$. The following remark gives a negative answer to this question (except the inclusion mentioned above) and the class $\mathcal{S}$ is thus in this sense as various as the class of all commutative radical rings.

Remark 2.4.15. For a ordered couple (A, B) of sets denote (I) the case when $A \subsetneqq B$, (II) the case when $A \supsetneqq B$ and (III) the case when $A = B$. Now consider following couples:

$(\mathcal{D}(S), \mathcal{N}(S))$: For (I) see 2.4.12 (with $k \in \mathbb{N}$). For (II) see 2.4.9. For (III) see 2.4.12 ($k = \infty$).

$(\mathcal{D}(S), \mathcal{T}(S))$: For (I) see 2.4.8(ii) (with $k \in \mathbb{N}$). For (II) see 2.4.9. For (III) see 2.3.8.

$(\mathcal{N}(S), \mathcal{T}(S))$: For (I) see 2.4.12 (with $k \in \mathbb{N}$). For (II) see 2.4.3 (with $\mathrm{char} F = 0$). For (III) see 2.4.3 (with $\mathrm{char} F > 0$) and 2.3.6.

$\mathcal{D}(S) \cap \mathcal{N}(S) \not\subseteq \mathcal{T}(S)$: See 2.4.9 ($\mathrm{char} F = 0$ with 2.4.7(i)).

$\mathcal{T}(S) \cap \mathcal{N}(S) \not\subseteq \mathcal{D}(S) \neq 0$: See 2.4.8(ii) ($i < k = \infty$ with 2.4.7(i)).

In the rest of this section we will deal with the annihilator.

The construction used for examples 2.3.6, 2.4.3, 2.4.8 and 2.4.12 forced an infinite annihilator (i.e. $\mathrm{Ann}(S) \cong \mathbb{Z}_{p^\infty}$) for a ring $S \in \mathcal{S}$ assuming that $\mathcal{T}(S) \neq S$. The following example shows that such assertion not true in general.

Example 2.4.16. Let $S(1, k) = p\mathbb{Z}_{p^k} \in \mathcal{S}$, where $k \geq 3$, be as in 2.3.6(i). Then $\mathrm{Ann}(S(1, k)) = \mathcal{M}(S(1, k)) \cong \mathbb{Z}_p$. Let $T = \big(\bigoplus_{k=3}^{\infty} S(1, k)\big)/I$ be the ring from the "gluing construction" (see 2.4.10). Put $\varphi : p\mathbb{Z} \to \mathit{End}(T(+))$, $\varphi(pk)(x) = pkx$, $x \in T$. Clearly, T is a $p\mathbb{Z}$-algebra (via φ). Then:

(i) $R = p\mathbb{Z} \oplus T$ is a subdirectly irreducible semiradical ring, $\mathcal{M}(R) = \mathcal{M}(T)$, $\mathcal{T}(R) \neq R$ and $\mathcal{D}(R) = 0$.

(ii) For $S = \mathcal{A}(R) \in \mathcal{S}$ we have $\mathcal{T}(S) \neq S$, $\mathcal{D}(S) = 0$ and $\mathrm{Ann}(S) = \mathcal{M}(S)$.

Proof. (i) First, we show that R is semiradical. Let $(pk, a) = (pk, a)(pl, b) = (p^2kl, pkb + pla + ab)$, where $k, l \in \mathbb{Z}$, $a, b \in T$. Then $pk = p^2kl$, thus $k = 0$. Hence we have $a = pla + ba$ and $(1 - pl)a = ba$. By induction, we get

$(1-pl)^n a = b^n a$ for every $n \in \mathbb{N}$. Hence $(1-pl)^{n_0} a = 0$ for some n_0, since T is a nil ring. But a is of order p^m for some $m \in \mathbb{N}_0$. Hence $a = 0$ and R is semiradical.

Now, we prove the R is subdirectly irreducible. Let $0 \neq x = (pk, a) \in R$. If $k \neq 0$ then, by the definition of T, there is $b \in T$ such that $ba = 0$ and the order of b is greater than $|pk|$. Then $(pk, a)(0, b) = (0, pkb) \neq 0$. Hence $R(0, a') + \mathbb{Z}(0, a') \subseteq Rx + \mathbb{Z}x$ for some $0 \neq (0, a') \in R$. Since T is subdirectly irreducible, by 2.4.10, we have $\mathcal{M}(T) \subseteq Ta' + \mathbb{Z}a' \subseteq R(0, a') + \mathbb{Z}(0, a') \subseteq Rx + \mathbb{Z}x$. The ring R is thus subdirectly irreducible.

Since T and $p\mathbb{Z}$ are reduced, R is also reduced.

(ii) Follows from (i). □

To have an infinite annihilator for $S \in \mathcal{S}$ we need of course $\mathcal{D}(S) \neq 0$. An easy observation can be made:

Let $S \in \mathcal{S}$. Assume that $\mathcal{T}(S) = S$ and $\mathcal{D}(S) \neq 0$. Since $\mathcal{D}(S) \cdot \mathcal{T}(S) = 0$, we get, by 2.1.1, that $\mathcal{D}(S) = \operatorname{Ann}(S) \cong \mathbb{Z}_{p^\infty}$, $p \in \mathbb{P}$.

In this case we have $\mathcal{D}(\mathcal{T}(S)) = \mathcal{D}(S) \neq 0$. By weakening this condition to $\mathcal{D}(\mathcal{T}(S)) \neq 0$, we can ask whether this assumption implies $\operatorname{Ann}(S) \cong \mathbb{Z}_{p^\infty}$ again. Indeed, for the previous examples 2.3.6, 2.4.3, 2.4.8, 2.4.12 and 2.4.16 is this conjecture true, but as the following example 2.4.17 shows, the general answer is negative again.

Example 2.4.17. Let a_1 be an element of order p in $\mathbb{Z}_{p^\infty}$. Put $U = (\mathbb{Z}_{p^\infty} \oplus \mathbb{Z}_{p^\infty})/K$, where K is a subgroup of $\mathbb{Z}_{p^\infty} \oplus \mathbb{Z}_{p^\infty}$ generated by $(a_1, -a_1)$. Let $T = p\mathbb{Z} \times p\mathbb{Z}$ be a product of rings. Put

$$\varphi : T \to End(U(+))$$

$$\varphi(pk, pl)\Big((a, b) + K\Big) = (pka, plb) + K,$$

for $(a, b) \in \mathbb{Z}_{p^\infty} \oplus \mathbb{Z}_{p^\infty}$. Clearly, U is a T-module. Further:

(i) $R = T \oplus U$ is a subdirectly irreducible semiradical ring, $\operatorname{Ann}(R) = \mathcal{M}(R) = (\mathbb{Z}_p \oplus \mathbb{Z}_p)/K$, and $\mathcal{T}(R) = U$ is a divisible group.

(ii) For $S = \mathcal{A}(R) \in \mathcal{S}$ we have $\mathcal{D}(\mathcal{T}(S)) = \mathcal{T}(S) \neq 0$ and $\operatorname{Ann}(S) = \mathcal{M}(S)$.

Proof. (i)First, for $0 \neq a \in U$ is clearly the order of a greater than the order of $(pk, pl)a$ for every $(pk, pl) \in U$. Hence R is semiradical by 2.4.11(i).

Now, let $0 \neq (pk, pl) \in T$. Obviously there are $a, b \in \mathbb{Z}_{p^\infty}$ such that at least one of the elements pka, plb is of order at least p^2. Then $(pk, pl) \cdot ((a, b) + K) \neq 0$. Hence U is a faithful T-module.

Finally, let $0 \neq (a, b) + K \in U$. Suppose that $(a, b) + K \notin M$, where $M = (\mathbb{Z}_p \oplus \mathbb{Z}_p)/K$. Then at least one of the orders of the elements a, b (say a) must be p^k, where $k \geq 2$. Hence $0 \neq (p^{k-1}, 0) \cdot ((a, b) + K) \in M$. Thus U is a subdirectly irreducible T-module with monolith M.

The rest follows by 2.4.11.

(ii) Easy by (i). □

2.5 Factors of the subdirectly irreducible radical rings by their monoliths

Having a subdirectly irreducible (universal) algebra, we can study the following natural question:

"Which algebras are homomorphic images of subdirectly irreducible algebras?"

T. Kepka asked for a characterization of those algebras in [17]. This question was answered by J. Ježek and T. Kepka in [11] and independently by D. Stanovský in [22] for the case of a variety of all algebras of a given signature with at least one at least binary operation. For varieties of all algebras with only unary operations was the problem partially solved in [12]. For the variety of semigroups was the complete answer given in [3]. In [21], the answer was given for quasigroups and groups. For lattices, an easy construction was found by Ralph Freese (unpublished).

In this section we study this question for the variety of (commutative) radical rings. We give some necessary conditions for such factors and make a characterization of the case when the factor is a zero-multiplication ring.

Proposition 2.5.1. *Let $S \in \mathcal{S}$. Then:*

(i) Every element of $S/\mathcal{M}(S)$ is a zero divisor.

(ii) If $S^2 \neq 0$ then $\mathrm{Ann}(S) \subsetneqq \mathcal{N}(S)$. In particular, if $S/\mathcal{M}(S) \neq 0$ then $\mathcal{N}(S/\mathcal{M}(S)) \neq 0$.

(iii) $\mathcal{T}(S/\mathcal{M}(S))$ is a p-group for some $p \in \mathbb{P}$ and $\mathrm{Ann}(S/\mathcal{M}(S)) \subseteq \mathcal{T}(S/\mathcal{M}(S))$.

(iv) $S/\mathcal{M}(S)$ is noetherian if and only if it is finite.

Proof. (i) Let $[0] \neq [a] \in S/\mathcal{M}(S)$. If $a \in \mathrm{Ann}(S)$, then $[a] \in \mathrm{Ann}(S/\mathcal{M}(S))$ and hence is a zero-divisor. If $a \notin \mathrm{Ann}(S)$, then there is $b \in S$ such that $0 \neq ba \in \mathcal{M}(S)$ and hence $[b] \cdot [a] = [0]$ and $[b] \neq [0]$ (otherwise would be $b \in \mathcal{M}(S) \subseteq \mathrm{Ann}(S)$ and $ba = 0$, a contradiction).

(ii) Let $a \in S \setminus \mathrm{Ann}(S)$. Suppose that $a \notin \mathcal{N}(S)$. Then $a^2 \notin \mathrm{Ann}(S)$ and hence there is $b \in S$ such that $0 \neq ba^2 \in \mathcal{M}(S) \subseteq \mathrm{Ann}(S)$. Thus $ba \in S \setminus \mathrm{Ann}(S)$ (otherwise $ba^2 = (ba)a = 0$, a contradiction) and $(ba)^2 = b(ba^2) = 0$. Therefore $ba \in \mathcal{N}(S) \setminus \mathrm{Ann}(S)$. Hence $\mathrm{Ann}(S) \subsetneqq \mathcal{N}(S)$.

(iii) By 2.1.1, $\mathcal{T}(S/\mathcal{M}(S))$ is a p-group. Now, if $[a] \in \mathrm{Ann}(S/\mathcal{M}(S))$, then $ra \in \mathcal{M}(S)$ for every $r \in R$. Since $\mathcal{M}(S) \cong \mathbb{Z}_p$ we have $r(pa) = p(ra) \in p\mathcal{M}(S) = 0$ for every $r \in S$ and hence $pa \in \mathrm{Ann}(S)$. The additive group $\mathrm{Ann}(S)$ is a p-group and thus $a \in \mathcal{T}(S)$.

(iv) Follows from 2.3.4. □

It is not difficult to see that considering $S \in \mathcal{S}$ from the examples 2.3.6, 2.4.3, 2.4.8 (with the semigroup taken from 2.4.7(i),(ii)), 2.4.12, 2.4.16 and 2.4.17, we have $\mathrm{Ann}(S/\mathcal{M}(S)) \neq 0$, provided that $S/\mathcal{M}(S) \neq 0$. Now we construct a subdirectly irreducible radical ring without this property (see 2.5.4).

First, we construct a semiradical semigroup A that will have slightly stronger properties than those ones in 2.4.6, namely

(i) $\mathrm{Ann}(A) = \{o, m\} \subsetneqq A$, where $m \neq o$.

(ii) $(\forall\, a \in A^*)(\exists\, b \in A)\; ab = m$.

(iii) For all $n \in \mathbb{N}$, $a_1, \dots, a_n \in A^*$ there exist $1 \leq i_0 \leq n$ and $b \in A$ such that $a_{i_0}b \in A^*$ and $a_ib = o$ for $a_i \neq a_{i_0}$.

Definition 2.5.2. Let A be a commutative semigroup with a zero element o is said to *have a basis $B \subseteq A^*$ (with respect to A^*)* iff every element $x \in A^*$ has (up to commutativity) unique form $x = b_1^{i_1} \cdots b_n^{i_n}$, where $n \in \mathbb{N}$, $b_k \in B$ are pairwise different and $i_k \in \mathbb{N}$ for $k = 1, \dots, n$.

Let $a, b \in A$. We say that a *divides* b if either $a = b$ or there is $c \in A$ such that $b = ac$.

Construction 2.5.3. Let A be a commutative semigroup with a zero element o and a basis $B \subseteq A^*$.

(1) Let F_X be a free commutative semigroup with a basis X. Put $F_X(A) = A \cup F_X \cup (A^* \times F_X)$ (a disjoin union of sets) and set a commutative binary operation $*$ on $F_X(A)$ as follows:

$$a * b = ab \qquad a * w = w * a = \begin{cases} o & , a \in \mathrm{Ann}(A) \\ (a, w) & , a \in A^* \end{cases}$$

$$u * w = uw \qquad a * (c, v) = (c, v) * a = \begin{cases} o & , ac \in \mathrm{Ann}(A) \\ (ac, v) & , ac \in A^* \end{cases}$$

$$u * (c, v) = (c, v) * u = (c, uv) \qquad (c, v) * (d, t) = \begin{cases} 0 & , cd \in \mathrm{Ann}(A) \\ (cd, vt) & , cd \in A^* \end{cases}$$

for $a, b \in A$, $u, w \in F_X$ and $(c, v), (d, t) \in A^* \times F_X$.

Then $F_X(A)$ is a commutative semigroup with a zero element o and a basis $B \cup X$, A is a subsemigroup of $F_X(A)$ and $\mathrm{Ann}(A) = \mathrm{Ann}(F_X(A))$.

Proof. Put $\widetilde{A} = A \cup \{1_A\}$ and $\widetilde{F} = F_X \cup \{1_F\}$, where 1_A and 1_F are new symbols (units), such that $a1_A = 1_Aa = a$, $1_A1_A = 1_A$ and $w1_F = 1_Fw = w$, $1_F1_F = 1_F$ for every $a \in A$, $w \in F_X$. Further denote $S = \widetilde{A} \times \widetilde{F}$ a product of semigroups, $W = (\mathrm{Ann}(A) \times F_X) \cup \{(o, 1_F)\}$ and $\rho = id_S \cup W \times W$ a relation on S. It is easy to see, that ρ is a congruence on S. Set $\varphi : F_X(A) \to S/\rho$, where $a \mapsto (a, 1_F)/\rho$, $w \mapsto (1_A, w)/\rho$ and $(a, w) \mapsto (a, w)/\rho$ with $a \in A$, $w \in F_X$, $(a, w) \in A^* \times F_X$. Now is easy to verify, that φ is a monomorphism and hence $F_X(A)$ is a semigroup.

Let $z = a_1 \dots a_n x_1 \dots x_k = a'_1 \dots a'_m x'_1 \dots x'_l \in A^* \times F_X$, where $n, m, k, l \geq 1$, $a_i, a'_j \in A$, $x_i, x'_j \in F_X$. Then $a_1 \dots a_n = a'_1 \dots a'_m$ and $x_1 \dots x_k = x'_1 \dots x'_l$. Hence, by assumption, z has an unique decomposition (up to commutativity) with respect to $B \cup X$. The rest is easy. □

(2) Suppose there is $o \neq m \in \mathrm{Ann}(A)$. Then there exists a commutative semigroup A' such that:

(i) A is a subsemigroup of A', o is a zero element in A' and $\mathrm{Ann}(A') = \mathrm{Ann}(A)$.

(ii) A' has a basis B' such that $B \subseteq B'$.

(iii) $(\forall\, a \in A^*)(\exists\, b \in A')\ ab = m$.

(iv) For all $n \in \mathbb{N}$, $a, a_1, \dots, a_n \in A^*$ such that a_i does not divide a for any $i = 1, \dots, n$ there exists $b \in A'$ such that $a_i b = 0$ for all $i = 1, \dots, n$ and $ab \in (A')^*$.

Proof. Set $X_1 = \{x_a | a \in A^*\}$, $X_2 = \{y_K | K \textit{ is a finite subset of } A^*\}$ (new symbols) and $X = X_1 \cup X_2$ (a disjoin union of sets). Now, let $F_X(A)$ be a semigroup as in (1). Further put $U = \{(a, x_a) | a \in A^*\}$, $V = \{(a, y_K) \in A^* \times X | K \textit{ is a finite subset of } A^*, a \in K\}$ and $Z = V \cup F_X(A) \cdot V \cup F_X(A) \cdot U$. By the definition of multiplication in $F_X(A)$, we have $U \cap Z = \emptyset$ and $m \notin Z$

It follows that $\sigma = id_{F_X(A)} \cup (U \times \{m\}) \cup (\{m\} \times U) \cup U \times U \cup Z \times Z$ is clearly a congruence on $F_X(A)$.

Put $A' = F_X(A)/\sigma$ and $\varphi : A \to F_X(A)/\sigma$, $a \mapsto [a] = a/\sigma$. Then φ is a monomorphism and A can be identified with a subsemigroup of A'.

(i) $\mathrm{Ann}(A') = \mathrm{Ann}(A)$: For $a \in A^*$ we obviously have $a \notin \mathrm{Ann}(A')$ and for $w \in F_X$ is also $[w] \notin \mathrm{Ann}(A')$, since $[w]^2 \neq [o]$.

Now, for $(a, w) \in A^* \times F_X$ such that $[(a, w)] \notin \mathrm{Ann}(A)$ suppose that $[(a, w)] \cdot [w] = [o]$. Then, by the definition of σ, $((a, w^2), o) \in Z \times Z$. Hence $(a, w^2) \in F_X(A) \cdot U \cup F_X(A) \cdot V$ and there is $z \in F_X(A)$ such that either $z(b, x_b) = (a, w^2)$ for some $(b, x_b) \in U$ or $z(c, y_K) = (a, w^2)$ for some $(c, y_K) \in V$, where K is finite subset of A^* and $c \in K$. Hence x_b (or y_K) divides w^2 and therefore, due to the basis of $F_X(A)$, x_b (or y_K) divides w. It follows that $(a, w) \in Z$ and thus $[(a, w)] = [o]$, a contradiction. Hence $[(a, w)] \cdot [w] \neq [o]$ and we have proved that $[(a, w)] \notin \mathrm{Ann}(A')$.

(ii) Put $B' = \varphi(B \cup X)$. Obviously $[x_a] \neq [x_b]$ for $a \neq b$. Now, if $[z_1 \dots z_n] = [z'_1 \dots z'_m] \notin \mathrm{Ann}(A')$ where $z_i, z'_j \in B \cup X$, then, since $[z] = [o]$ for every $z \in Z$, we have, by the definition of σ, that $z_1 \dots z_n = z'_1 \dots z'_m$. Hence the decomposition is unique, since $B \cup X$ is a basis of $F_X(A)$.

(iii) For $[a] = a \in A^*$ we have $[a] \cdot [x_a] = [m] = m$, where $x_a \in X_1$.

(iv) Let $a \in A^*$ and $K = \{a_1, \dots, a_n\} \subseteq A^*$, $n \in \mathbb{N}$, be such that a_i doesn't divide a for any $i = 1, \dots, n$. Then, obviously, $[a_i] \cdot [y_K] = [o]$. Suppose now, for contradiction, that $[(a, y_K)] \in \mathrm{Ann}(A')$. Then $[(a, y_K^2)] = [0]$. Hence, by the definition of σ, $((a, y_K^2), o) \in Z \times Z$. Thus $(a, y_K^2) \in F_X(A) \cdot V$. Due to the multiplication in $F_X(A)$ and the basis B', we get that either $(a, y_K^2) = y_K(a, y_K)$, where $(a, y_K) \in V$, or $(a, y_K^2) = (b, y_K)(c, y_K)$, where $(c, y_K) \in V$. In the first case we get $a \in K$ and in the second case we have $c \in K$ and $a = cb$ for $b \in A$. Hence there is $1 \leq i \leq n$ such that $a_i \in K$ divides a, a contradiction. □

(3) There is a (countable) commutative semigroup A_1 with a zero element o such that:

(i) $\mathrm{Ann}(A_1) = \{o, m\} \subsetneq A_1$, where $m \neq o$.

(ii) A_1 is semiradical.

(iii) $(\forall\, a \in A_1^*)(\exists\, b \in A_1)\; ab = m$.

(iv) For all $n \in \mathbb{N}$, $a_1, \dots, a_n \in A_1^*$ there exist $1 \leq i_0 \leq n$ and $b \in A_1$ such that $a_{i_0} b \in A_1^*$ and $a_i b = o$ for $a_i \neq a_{i_0}$.

Proof. Let $D_0 = \{0, m\}$, $m \neq 0$ be a zero multiplicative semigroup, $X = \{x\}$. Put $D_1 = F_X(D_0)$. Further, by the induction, set $D_{n+1} = (D_n)'$ (see (2)) for $n \in \mathbb{N}$. Now, put $A_1 = \bigcup_n D_n$. Let B_n be the appropriate bases for D_n, $n \in \mathbb{N}$. Since D_1 is infinite, we have, by the proof of (2), that B_2 is also infinite. Now, clearly, A_1 has an infinite basis $B = \bigcup_n B_n$. Finally, for all $n \in \mathbb{N}$, $a, a_1, \dots, a_n \in A_1^*$ such that a_i does not divide a for any $i = 1, \dots, n$ there exists $b \in A_1$ such that $a_i b = 0$ for all $i = 1, \dots, n$ and $ab \in A_1^*$.

(i) and (iii). Obvious.

(ii) Let $o \neq a \in A_1$ such that $ab = a \neq o$ for some $b \in A_1$. Then $a, b \notin \mathrm{Ann}(A_1)$ and hence there are two different decomposition of a in the basis B, a contradiction. Hence A_1 is semiradical.

(iv) Let $n \in \mathbb{N}$ and $a_1, \dots, a_n \in A_1^*$ be pair-wise different elements.

First, suppose that $n = 1$. Since B is infinite, there is $b_0 \in B$ that does not divide a_1. Hence, by the property of A_1, we have $c = a_1 b \in A_1^*$ and $b_0 b = o$ for some $b \in A_1$.

Now, let $n \geq 2$. Then there is i_0 such that a_i doesn't divide a_{i_0} for every $i \neq i_0$. Indeed, suppose on the contrary, that there is a map $\varphi : \{1, \dots, n\} \to \{1, \dots, n\}$ such that $a_i = b_i a_{\varphi(i)}$ for every i, where $b_i \in S$. Then, by 2.2.12, $\varphi^k(i') = i'$ for some $i' \in \{1, \dots, n\}$ and $k \in \mathbb{N}$. Hence $a_{i'} = b_{i'} a_{\varphi(i')} = b_{i'} b_{\varphi(i')} a_{\varphi^2(i')} = \cdots = b_{i'} \dots b_{\varphi^{k-1}(i')} a_{\varphi^k(i')}$, a contradiction with the semiradicality of A_1.

Now, again, by the property of A_1, we have that there exists $b \in A_1$ such that $a_{i_0} b \in A_1^*$ and $a_i b = o$ for $a_i \neq a_{i_0}$. □

Now we find the desired counterexample.

Example 2.5.4. Let A_1 be the semigroup constructed in 2.5.3 (3) with a zero element o and $\mathrm{Ann}(D) = \{o, m\}$, $m \neq o$. Let p be a prime number. Let $R = (\mathbb{Z}_p)_0[A_1]$ be the contracted semigroup algebra. Then:

(i) R is a subdirectly irreducible semiradical ring and $\mathcal{M}(R) = \mathbb{Z}_p \cdot m = \operatorname{Ann}(R)$.

(ii) For every $x \in R \setminus \operatorname{Ann}(R)$ there is $y \in R$ such that $xy \in R \setminus \operatorname{Ann}(R)$.

(iii) $S = \mathcal{A}(R) \in \mathcal{S}$, $\operatorname{Ann}(S) = \mathcal{M}(S)$ and $\operatorname{Ann}(S/\mathcal{M}(S)) = 0$.

Proof. (i) and (ii). Let $x \in R \setminus \mathbb{Z}_p \cdot m$. We show that $xb = \mu c$ for some $0 \neq \mu \in \mathbb{Z}_p$, $b \in A_1$ and $c \in A_1^*$.

Clearly, $x = \sum_{i=1}^{n} \lambda_i a_i + \lambda m$, where $n \geq 1$, $\lambda, \lambda_i \in \mathbb{Z}_p$, $a_i \in A_1^*$, $\lambda_i \neq 0$ for all $i = 1, \dots, n$ and $a_i \neq a_j$ for $i \neq j$. By 2.5.3(3)(iv), there exist $1 \leq i_0 \leq n$ and $b \in A_1$ such that $a_i b = 0$ for $i \neq i_0$ and $c = a_{i_0} b \in A_1^*$. Hence $xb = \lambda_{i_0} a_{i_0} b = \lambda_{i_0} c$.

Since $xb \neq 0$, we have $x \in R \setminus \operatorname{Ann}(R)$ and we have proved that $\operatorname{Ann}(R) \subseteq \mathbb{Z}_p \cdot m$. The other inclusion is trivial. Hence $\operatorname{Ann}(R) = \mathbb{Z}_p \cdot m = \mathcal{M}(R)$ and $xb \in R \setminus \operatorname{Ann}(R)$.

The rest follows from by 2.2.13(ii).

(iii) Follows from 2.2.8, (i) and (ii). □

In the rest we classify such zero-multiplication rings that are isomorphic to $S/\mathcal{M}(S)$ for some $S \in \mathcal{S}$.

Construction 2.5.5. Let $G(+)$ be a commutative group, $p \in \mathbb{P}$, $\mu : G \times G \to \mathbb{Z}_p$ be a symmetric bi-additive form such that $0 \neq \ker(\mu)\{x \in S | (\forall a \in S)(\mu(x, a) = 0)\} \subseteq \mathbb{Z}_{p^\infty}$ and $0 \neq m \in \ker(\mu)$ be an element of order p. Put $\mathcal{S}(G, \mu, m) = G$ and set the following multiplication $a \cdot b = \mu(a, b)m$ for $a, b \in G$. Then:

(i) $S = \mathcal{S}(G, \mu, m) \in \mathcal{S}$, $\mathcal{M}(S) = \mathbb{Z}_p \cdot m$ and $\operatorname{Ann}(S) = \ker(\mu)$.

(ii) $S/\mathcal{M}(S)$ is a zero-multiplication ring.

Proof. First we show the associativity of the multiplication. For $a, b, c \in S$ we have $(ab)c = (\mu(a, b)m)c = \mu(\mu(a, b)m, c)m = 0$, since $m \in \ker(\mu)$ and hence $a(bc) = (bc)a = 0 = (ab)c$. The distributivity is easy to verify. Further put $\widetilde{a} = -a + \mu(a, a)m$ for $a \in S$. Then $a + \widetilde{a} + a\widetilde{a} = a + (-a + \mu(a, a)m) + \mu(a, -a + \mu(a, a)m)m = \mu(a, a)m - \mu(a, a)m + \mu(a, \mu(a, a)m)m = 0$ and hence S is a radical ring.

For $a \in S \setminus \ker(\mu)$ there is $b \in S$ such that $ba = \mu(a, b)m \neq 0$ and for $a \in \ker(\mu)$ there is $k \geq 0$ such that $p^k a = m$, thus S is a subdirectly irreducible with a monolith $\mathbb{Z}_p \cdot m$. The rest is clear. □

Proposition 2.5.6. *Let $S \in \mathcal{S}$ be such that $S/\mathcal{M}(S)$ is a zero-multiplication ring. Then there are $p \in \mathbb{P}$, a bi-additive symmetric form $\mu : S \times S \to \mathbb{Z}_p$ and $0 \neq m \in \mathcal{M}(S)$ such that $S \cong \mathcal{S}(G, \mu, m)$.*

Proof. Let $\mathcal{M}(S) \cong \mathbb{Z}_p$. Take $0 \neq m \in \mathcal{M}(S)$. Since $S/\mathcal{M}(S)$ is a a zero-multiplication ring, we have $S^2 \subseteq \mathcal{M}(S)$. Now, just set $\mu(a, b) = \lambda$, where $ab = \lambda m$, $a, b \in S$. The rest is clear. □

Lemma 2.5.7. *Let $G(+)$ be a commutative group, $p \in \mathbb{P}$, $\mu : G \times G \to \mathbb{Z}_p$ be a symmetric bi-additive form such that $0 \neq \ker(\mu)\{x \in S | (\forall a \in S)(\mu(x, a) = 0)\} \subseteq \mathbb{Z}_{p^\infty}$ and $0 \neq m \in \ker(\mu)$ be an element of order p.*

Then $G = H \oplus K$, where H and K are subgroups of G such that $pH = 0$ and either $K = \ker(\mu)$ (in this case $pG = p\ker(\mu)$) or $K \cong \mathbb{Z}_{p^k}$ for some $2 \leq k \in \mathbb{N}$ and $pK = \ker(\mu)$ (in this case $p\ker(\mu) \subsetneqq pG = \ker(\mu)$).

Proof. We have $p\ker(\mu) \subseteq pG \subseteq \ker(\mu) \subseteq \mathbb{Z}_{p^\infty}$ since $\mu(pa, x) = p\mu(a, x) = 0$ for all $a, x \in G$. Hence $\ker(\mu) \cong \mathbb{Z}_{p^n}$, where $1 \leq n \leq \infty$. If $n = \infty$ then $p\ker(\mu) = pG = \ker(\mu)$ and we put $K = \ker(\mu)$. If $n \in \mathbb{N}$, then either $p\ker(\mu) = pG$ (and we put $K = \ker(\mu)$ again) of $p\ker(\mu) \subsetneqq pG = \ker(\mu)$ and then there is an element $a \in G$ of order p^{n+1}. In the later case we put $K = \langle a \rangle$ and we have $pK = \ker(\mu)$.

Hence we always have $pG = pK$. Now, there obviously is a group $H \subseteq Soc(G)$ such that $Soc(G) = H \oplus (K \cap Soc(G))$.

We show that $G = H \oplus K$. Obviously, $H \cap K = H \cap K \cap Soc(G) = 0$. Let $x \in G$. Since $pK = pG$, there is $b \in K$ such that $px = pb$ and hence $x = b + (x - b) \in K + H$. □

Corollary 2.5.8. *A zero-multiplication ring R is isomorphic to $S/\mathcal{M}(S)$ for some $S \in \mathcal{S}$ if and only if $R(+) \cong (\mathbb{Z}_p)^{(\kappa)} \oplus \mathbb{Z}_{p^n}$, with $p \in \mathbb{P}$, κ an ordinal number and $1 \leq n \leq \infty$.*

Proof. ($\Rightarrow$) Follows from 2.5.6, 2.5.7 and 2.5.5, since the monolith is contained in the annihilator.

($\Leftarrow$) Let $R(+) \cong (\mathbb{Z}_p)^{(\kappa)} \oplus F$, where $F = \mathbb{Z}_{p^n}$, $1 \leq n \leq \infty$. If $n = \infty$ put $K = F$ and if $n < \infty$ put $K = \mathbb{Z}_{p^{n+1}}$. Now, set $G = (\mathbb{Z}_p)^{(\kappa)} \oplus K$. Let $\{e_\alpha | \alpha < \kappa\}$ be a basis of $(\mathbb{Z}_p)^\kappa$. Set $\mu(\sum_\alpha \lambda_\alpha e_\alpha + a, \sum_\beta \mu_\beta e_\beta + b) = \sum_\alpha \lambda_\alpha \mu_\alpha$ for $\lambda_\alpha, \mu_\beta \in \mathbb{Z}_p$ and $a, b \in F$. Let $m \in F$ be a element of order p. Now, by 2.5.5, $R \cong S/\mathcal{M}(S)$, where $S = \mathcal{S}(G, \mu, m) \in \mathcal{S}$. □

The previous classification gives us a hint to find an example of a finite radical ring, that cannot be isomorphic to any factor of a subdirectly irreducible radical ring by its monolith.

Example 2.5.9. Let $R = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$ be a zero-multiplication ring. Then R is radical, but there is no $S \in \mathcal{S}$ such that $S/\mathcal{M}(S) \cong R$.

Indeed, suppose that $\varphi : S \to R$ is such an epimorphism. Then $\psi : S/Soc(S) \to R/Soc(R)$, $\psi(x + Soc(S)) = \varphi(x) + Soc(R)$ is also an epimorphism, where $Soc(G) = \{a \in G | pa = 0\}$ is the socle for a p-group G. But $S/Soc(S)$ is cyclic by 2.5.6 and 2.5.8, while $R/Soc(R) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, a contradiction.

The further classification of factors (the nilpotent case for instance) seems to be quite difficult at this point. Remark, that even for commutative rings with unit no similar classification was done yet.

Chapter 3

Subsemirings of rational numbers

3.1 Introduction

A (commutative) *semiring* is an algebraic structure with two commutative and associative binary operations (an addition and a multiplication) such that the multiplication distributes over the addition. Although the literature concerning semirings is not so voluminous as for the rings, several sources can be found in the books [6], [7], [8], [9] and [10].)

Under a homomorphism of semirings we will understand a map that preserves addition and multiplication. In this chapter a ring may be with or without unit.

For a semirings S and a subset $X \subseteq S$ we denote $\langle X \rangle$ the subsemiring generated by X.

For all $p \in \mathbb{P}$ and $q \in \mathbb{Q}^*$, there exists a uniquely determined integer $\mathrm{v}_p(q)$ such that $q = \pm \prod_{p \in \mathbb{P}} p^{\mathrm{v}_p(q)}$; (of course, only finitely many of the numbers $\mathrm{v}_p(q)$ are non-zero).

The map $\mathrm{v}_p : \mathbb{Q}^* \to \mathbb{Z}$ for a prime p has the usual properties of a valuation:

(i) $\mathrm{v}_p(-r) = \mathrm{v}_p(r)$,

(ii) $\mathrm{v}_p(rs) = \mathrm{v}_p(r) + \mathrm{v}_p(s)$,

(iii) $\mathrm{v}_p(r+s) \geq \min(\mathrm{v}_p(r), \mathrm{v}_p(s))$, provided that $r \neq -s$,

(iv) $\mathrm{v}_p(r+s) = \min(\mathrm{v}_p(r), \mathrm{v}_p(s))$, provided that $\mathrm{v}_p(r) \neq \mathrm{v}_p(s)$

for every $r, s \in \mathbb{Q}^*$.

In the beginning notice, that every subsemiring of $\mathbb{Q}$ is either contained in $\mathbb{Q}_0^+$ or is a ring (see 3.1.1).

Proposition 3.1.1. *Let S be a subsemiring of $\mathbb{Q}$ such that $S \cap \mathbb{Q}^- \neq \emptyset$. Then S is a subring of $\mathbb{Q}$.*

Proof. If $x \in S \cap \mathbb{Q}^-$, then $x^2 \in S \cap \mathbb{Q}^+$, Now it is enough to show that every subsemigroup of $\mathbb{Q}(+)$, that contains at least one positive and at least one negative element, is a group.

Indeed, let $a, b, c, d \in \mathbb{N}$ be such that $a/b \in S$ and $-c/d \in S$. Then $bc - 1 \in \mathbb{N}_0, ad \in \mathbb{N}$ and hence, $-a/b = (bc-1)a/b + ad(-c/d) \in S$. Similarly, $bc \in \mathbb{N}, ad - 1 \in \mathbb{N}_0$ and $c/d = bc(a/b) + (ad-1)(-c/d) \in S$.

Thus S is a subring. □

Now we recall the well known classification of subrings (not necessary with unit) of $\mathbb{Q}$ (for more details see for instance [16]). For a non-zero subring A of $\mathbb{Q}$ denote $\chi(A) = \min(A \cap \mathbb{N})$.

Proposition 3.1.2. [16, 10.4] *There exists a bi-unique correspondence between (non-zero) subrings of $\mathbb{Q}$ and ordered pairs (P, m), where $m \in \mathbb{N}$ and P is a subset of $\mathbb{P}$ such that $p \in \mathbb{P} \setminus P$ whenever $p \in \mathbb{P}$ divides m.*

If A is a subring of $\mathbb{Q}$, then the corresponding pair is $(\mathtt{p}_A, \chi(A))$, where $\mathtt{p}_A = \{p \in \mathbb{P} |\ \chi(A)/p \in A\}$.

If (P, m) is a pair as above, then the corresponding subring is $\mathrm{A}_{(P,m)} = \{q \in \mathbb{Q}^* | \mathrm{v}_p(q) \geq \mathrm{v}_p(m) \text{ for every } p \in \mathbb{P} \setminus P\} \cup \{0\}$. Moreover:

(i) If A_1 and A_2 are subrings of $\mathbb{Q}$, then $A_1 \subseteq A_2$ if and only if $\chi(A_2)$ divides $\chi(A_1)$ and $\mathtt{p}_{A_1} \subseteq \mathtt{p}_{A_2}$ and $A_1 \cong A_2$ if and only if $A_1 = A_2$.

(ii) If A is a subring of $\mathbb{Q}$, then A is a finitely generated ring if and only if the set $\mathtt{p}_A$ is finite.

Moreover, there is a classification for the unitary subring of $\mathbb{Q}$ too.

Proposition 3.1.3. [16, 10.2] *There exists a bi-unique correspondence between unitary subrings of $\mathbb{Q}$ and subsets of $\mathbb{P}$.*

If A is a unitary subring of $\mathbb{Q}$, then the corresponding subset is $\mathtt{p}_A = \{p \in \mathbb{P} |\ 1/p \in A\}$.

If P is a subset of $\mathbb{P}$, then the corresponding unitary subring is $\mathrm{A}_P = \{q \in \mathbb{Q}^* | \mathrm{v}_p(q) \geq 0 \text{ for every } p \in \mathbb{P} \setminus P\} \cup \{0\}$. Moreover:

(i) If A_1 and A_2 are unitary subrings of $\mathbb{Q}$, then $A_1 \subseteq A_2$ if and only if $\mathtt{p}_{A_1} \subseteq \mathtt{p}_{A_2}$ and $A_1 \cong A_2$ if and only if $A_1 = A_2$.

(ii) If A is a unitary subring of $\mathbb{Q}$, then A is a finitely generated ring if and only if the set $\mathtt{p}_A$ is finite.

(iii) $\mathtt{p}_{\mathbb{Z}} = \emptyset$.

(iv) $\mathtt{p}_{\mathbb{Q}} = \mathbb{P}$.

Since any subsemiring of $\mathbb{Q}_0^+$ can be assumed (without loss of generality) to be without zero, the classification of all subsemirings of $\mathbb{Q}$ means now to classify subsemirings of $\mathbb{Q}^+$.

The following remark says that different subsemirings of $\mathbb{Q}$ are non-isomorphic. For the classification this means to find just all subsemirings of $\mathbb{Q}^+$, which is a quite big task, since, as we will see, this class is much more colorful, complicated and relatively bigger than the class of subrings of $\mathbb{Q}$.

Remark 3.1.4. Let S_1 and S_2 be subsemirings of $\mathbb{Q}$ and let $\varphi : S_1 \to S_2$ be a homomorphism (i.e., φ is a mapping such that $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in S_1$).

(i) First, assume that $S_1 \subseteq \mathbb{N}_0$. If $0 \in S_1$, then $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$, so that $\varphi(0) = 0 \in S_2$. If $m \in S_1 \backslash \{0\}$ then $\varphi(m)\varphi(m) = \varphi(m^2) = m\varphi(m)$, and hence either $\varphi(m) = 0$ or $\varphi(m) = m$. If $m, n \in S_1 \backslash \{0\}$ are such that $\varphi(m) = 0$ and $\varphi(n) \neq 0$, then $\varphi(n) = n, \varphi(m+n) = \varphi(n) = n \neq 0$, and hence $\varphi(m+n) = m+n$ and $m = 0$, a contradiction. We have shown that either $0 \in S_2$ and $\varphi = 0$ or $S_1 \subseteq S_2$ and $\varphi = \mathrm{id}_{S_1}$.

(ii) Next, assume that $S_1 \subseteq \mathbb{Q}_0^+$. Again, if $0 \in S_1$, then $\varphi(0) = 0$. If $a/b \in S_1$, $a, b \in \mathbb{N}$, then $a = b \cdot a/b \in T = S_1 \cap \mathbb{N}$ and $\varphi(a) = b\varphi(a/b), \varphi(a/b) = \varphi(a)/b$. Put $\psi = \varphi \restriction_T$. According to (i), either $0 \in S_2$ and $\psi = 0$ or $T \subseteq S_2$ and $\psi = \mathrm{id}_T$. In the former case, we get $\varphi(a) = 0$ and $\varphi(a/b) = 0$. In the latter case, we get $\varphi(a) = a$ and $\varphi(a/b) = a/b$. We have thus shown again that either $0 \in S_2$ and $\varphi = 0$ or $S_1 \subseteq S_2$ and $\varphi = \mathrm{id}_{S_1}$.

(iii) Assume, finally, that $S_1 \nsubseteq \mathbb{Q}_0^+$. By 3.1.1, S_1 is a subring of $\mathbb{Q}$. If $a \in S_1 \cap \mathbb{Q}^-$, then $-a \in S_1 \cap \mathbb{Q}^+$ and $0 = \varphi(a-a) = \varphi(a) + \varphi(-a)$ and $\varphi(a) = -\varphi(-a)$. Using (ii), we see that either $0 \in S_2$ and $\varphi = 0$ or $S_1 \subseteq S_2$ and $\varphi = \mathrm{id}_{S_1}$.

(iv) Combining (ii) and (iii), we conclude that either $0 \in S_2$ and $\varphi = 0$ or $S_1 \subseteq S_2$ and $\varphi = \mathrm{id}_{S_1}$.

(v) It follows immediately from (iv) that different subsemirings of $\mathbb{Q}$ are non-isomorphic.

3.2 First approach to subsemirings of $\mathbb{Q}^+$

Throughout this section, let S be a subsemiring of $\mathbb{Q}^+$.

First, we look into the behaviour of S with respect to the valuation v_p and to the interval $(0,1)$.

Lemma 3.2.1. *Let $p \in \mathbb{P}$. Then either there exists $m \in \mathbb{N}_0$ such that $\mathrm{v}_p(S) = \{m, m+1, \dots\}$ or $\mathrm{v}_p(S) = \mathbb{Z}$.*

Proof. Let $a \in S$. First, suppose $\mathrm{v}_p(a) = k \geq 0$ and $k \leq n \in \mathbb{N}_0$. Then $p^{n-k}a \in S$ and $\mathrm{v}_p(p^{n-k}a) = n-k+k = n$.

Now, let $\mathrm{v}_p(a) = -k < 0$ and $n \in \mathbb{Z}$. Then $b = p^{k-1}a \in S$ and $\mathrm{v}_p(b) = -1$. For $n \geq 0$ we have $x = p^{n+1}b \in S$ and $\mathrm{v}_p(x) = n$. For $-n < 0$ we have $x = b^n \in S$ and $\mathrm{v}_p(x) = n$.

The assertion follows now easily. □

Lemma 3.2.2. [2, 9.4] *Let $a, b, c, d \in \mathbb{N}$ be such that $a < b$, $c < d$ and $\gcd(a,b) = \gcd(c,d) = \gcd(a,c) = 1$. Then $1/\mathrm{lcm}(b,d) \in \langle a/b, c/d \rangle$.*

Lemma 3.2.3. *Let $m \in \mathbb{N}$. Let $p_1, \dots, p_m$ be pairwise different prime integers and let $a_1, \dots, a_m \in S \cap (0,1)$ be such that $\mathrm{v}_{p_i}(a_i) \leq 0$ for every $1 \leq i \leq m$.*

Then there is $b \in S \cap (0,1)$ such that $\mathrm{v}_{p_i}(b) \leq 0$ for all $i = 1, \dots, m$.

Proof. First of all, find an integer n such that $m < n$ and $a_i^n < 1/\big(m(p_1 \dots p_m)^m\big)$, for every $i = 1, 2, \dots, m$. Put $b_i = (p_1 \dots p_{i-1}p_{i+1} \dots p_m)^i a_i^n$ and $b = \sum_i b_i$. We have $b_i < (p_1 \dots p_m)^i a_i^n \leq (p_1 \dots p_m)^m a_i^m < 1/m$ and $b < 1$. Clearly, $b \in \langle a_1, \dots, a_m \rangle \subseteq S$. Moreover, $\mathrm{v}_{p_i}(b_i) = n\mathrm{v}_{p_i}(a_i) \leq 0$ and $\mathrm{v}_{p_i}(b_j) = n\mathrm{v}_{p_i}(a_j) + j$ for $j \neq i$. If $\mathrm{v}_{p_i}(b_{j_1}) = \mathrm{v}_{p_i}(b_{j_2})$ for $j_1 < j_2$, $j_1 \neq i \neq j_2$, then $n(\mathrm{v}_{p_i}(a_{j_1}) - \mathrm{v}_{p_i}(a_{j_2})) = j_2 - j_1$, $1 \leq j_2 - j_1 < m$, a contradiction with $m < n$. Similarly, if $\mathrm{v}_{p_i}(b_i) = \mathrm{v}_{p_i}(b_j)$ for $i \neq j$, then $n(\mathrm{v}_{p_i}(a_i) - \mathrm{v}_{p_i}(a_j)) = j$, $1 \leq j < m$, again a contradiction. We see that the numbers $\mathrm{v}_{p_i}(b_1), \dots, \mathrm{v}_{p_i}(b_m)$ are pair-wise different, and hence $\mathrm{v}_{p_i}(b) = \min\{\mathrm{v}_{p_i}(b_j) | 1 \leq j \leq m\} \leq \mathrm{v}_{p_i}(b_i) \leq 0$. □

As we see, the set $S \cap (0,1)$ together with the primes p such that $\mathrm{v}_p(S) = \mathbb{Z}$ play an important role in the structure of S.

Definition 3.2.4. Put

$$\mathtt{p}(S) = \{p \in \mathbb{P} | \mathrm{v}_p(S) = \mathbb{Z}\}.$$

(That is, $p \in \mathtt{p}(S)$ if and only if $\mathrm{v}_p(a) < 0$ for at least one $a \in S$.)

Let $p \in \mathbb{P}$. A semiring S will be called *p-paradivisible* if $S \cap (0,1) \neq \emptyset$ and $\mathrm{v}_p(a) > 0$ for every $a \in S \cap (0,1)$.

We denote by $\mathtt{pd}(S)$ the set of all $p \in \mathbb{P}$ such that S is p-paradivisible.

Remark 3.2.5. Let S_1 and S_2 be subsemirings of $\mathbb{Q}^+$ such that $S_1 \subseteq S_2$. Then $\mathtt{p}(S_1) \subseteq \mathtt{p}(S_2)$. Moreover, if $S_1 \cap (0,1) \neq \emptyset$, then $\mathtt{pd}(S_2) \subseteq \mathtt{pd}(S_1)$.

Lemma 3.2.6. *Let $S \cap (0,1) \neq \emptyset$. If $p \in \mathtt{p}(S)$ is such that S is not p-paradivisible, then there exists $x \in S \cap (0,1)$, such that $\mathrm{v}_p(x) < 0$.*

Proof. Since $p \in \mathtt{p}(S)$, there exists $x' \in S$, such that $\mathrm{v}_p(x') < 0$. Suppose that $x' \geq 1$ (otherwise we are done). Since $S \cap (0,1) \neq \emptyset$ and S is not p-divisible, there exists $y \in S$, such that $0 < y < 1$ and $\mathrm{v}_p(y) \leq 0$. Hence $0 < y^n x' < 1$ and $\mathrm{v}_p(y^n x') < 0$ for suitable $n \in \mathbb{N}$ and we can put $x = y^n x'$. □

Proposition 3.2.7. *Assume that $S \cap (0,1) \neq \emptyset$ and that $\mathtt{pd}(S) = \emptyset$.*

Then $S = \left\langle \{\frac{1}{p} | p \in \mathtt{p}(S)\} \right\rangle = \{x \in \mathbb{Q}^+ | \big(\forall\, q \in \mathbb{P} \setminus \mathtt{p}(S)\big)\ \mathrm{v}_q \geq 0\}$.

Proof. Set $\widetilde{S} = \left\langle \{\frac{1}{p} | p \in \mathtt{p}(S)\} \right\rangle$. The inclusion $S \subseteq \widetilde{S}$ is obvious.

$\widetilde{S} \subseteq S$: We show that if $p \in \mathtt{p}(S)$ then $1/p \in S$. By 3.2.6, there is $\frac{a}{b} \in S \cap (0,1)$, such that p does not divide a but divides b. Let $a = p_1^{k_1} \dots p_n^{k_n}$ be composition into powers of primes. By assumption, for every p_i there is $x_i \in S \cap (0,1)$ such that $\mathrm{v}_{p_i}(x_i) \leq 0$. Using 3.2.3, there exists $c/d \in S \cap (0,1)$ such that p_i does not divide c for all i. Now, by 3.2.2, follows that $1/s \in S$, where s is the least common multiple of b and d. Hence p divides s and therefore $1/p = k(1/s) \in S$ for suitable $k \in \mathbb{N}$.

The rest is obvious. □

Now we have fully classified those subsemirings that are not p-paradivisible for any prime p and have a non-empty intersection with the interval $(0,1)$. For a better understanding of the remaining ones we need another notion. A suitable machinery will be introduced in the next section.

3.3 Characteristic sequences

Throughout this section, again, let S be a subsemiring of $\mathbb{Q}^+$.

Denote $\bar{\mathbb{R}}_0^+ = \mathbb{R}_0^+ \cup \{\infty\}$ the set of positive reals together with "∞" and equipped with the standard topology, ordering and algebraic structure, where $a \leq \infty$ and $a + \infty = \infty + a = \infty + \infty = a \cdot \infty = \infty \cdot a = \infty \cdot \infty = \infty$ for every $a \in \mathbb{R}_0^+$ (i.e. ∞ is the greatest element and absorbing element for both operations).

We start with assigning of characteristic sequences to S. All operations and ordering on sequences are supposed to be component-wise.

Definition 3.3.1. For $n \in \mathbb{Z}$ and $p \in \mathbb{P}$ we put

$$\mathbf{u}_n(S,p) = \begin{cases} \inf\{x \in S | \mathrm{v}_p(x) \leq n\} & , \ n \in \mathrm{v}_p(S) \\ \infty & , \ n \notin \mathrm{v}_p(S). \end{cases}$$

We call the sequence $\boldsymbol{u}(S,p) = (\mathbf{u}_n(S,p))_{n\in\mathbb{Z}} \subseteq \bar{\mathbb{R}}_0^+$ a *characteristic p-sequence* of a semiring $S \subseteq \mathbb{Q}^+$.

Further denote $\boldsymbol{e}_{(\infty,0)} = (e_n)_{n\in\mathbb{Z}} \subseteq \bar{\mathbb{R}}_0^+$ a sequence such that

$$e_n = \begin{cases} \infty & , \ n < 0 \\ 0 & , \ n \geq 0. \end{cases}$$

Remark 3.3.2. Let $p \in \mathbb{P}$. Let $S_1 \subseteq S_2$ be subsemirings of $\mathbb{Q}^+$. Then $\boldsymbol{u}(S_2,p) \leq \boldsymbol{u}(S_1,p)$.

The following proposition gathers the basic properties of p-characteristic sequences.

Proposition 3.3.3. *Let $n, m \in \mathbb{Z}$ and $p \in \mathbb{P}$. Then:*

(i) $n \leq m \quad \Rightarrow \quad \mathbf{u}_m(S,p) \leq \mathbf{u}_n(S,p)$.

(ii) $\mathbf{u}_{n+m}(S,p) \leq \mathbf{u}_n(S,p) \cdot \mathbf{u}_m(S,p)$.

Proof. (i) Follows easily by 3.2.1.

(ii) First, suppose that $\mathbf{u}_{n+m}(S,p) = \infty$. Then, by definition and 3.2.1, $\mathrm{v}_p(S) \subseteq \mathbb{N}_0$. Hence $m + n < d = \min \mathrm{v}_p(S)$ and it follows that either $m < d$ or $n < d$. Thus $\mathbf{u}_m(S,p) = \infty$ or $\mathbf{u}_n(S,p) = \infty$ and our assertion is true.

Now, we can assume without loss of generality, that all the three members in the inequality are finite. By definition, there exist sequences

$(x_k)_{k\in\mathbb{N}}, (y_k)_{k\in\mathbb{N}} \subseteq S$ such that $\mathrm{v}_p(x_k) \leq n$, $\mathrm{v}_p(y_k) \leq m$ for every $k \in \mathbb{N}$ and $x_k \overset{k\to\infty}{\longrightarrow} \mathbf{u}_n(S,p)$ and $y_k \overset{k\to\infty}{\longrightarrow} \mathbf{u}_m(S,p)$. Hence $\mathrm{v}_p(x_k y_k) \leq n+m$ and $\mathbf{u}_{n+m}(S,p) \leq x_k y_k \overset{k\to\infty}{\longrightarrow} \mathbf{u}_n(S,p) \cdot \mathbf{u}_m(S,p)$. □

Proposition 3.3.4. *Assume $S \cap (0,1) \neq \emptyset$. Then there is a finite subset $K \subseteq \mathbb{P}$ such that either $\boldsymbol{u}(S,p) = 0$ or $\boldsymbol{u}(S,p) = \boldsymbol{e}_{(\infty,0)}$ for every $p \in \mathbb{P} \setminus K$.*

Proof. Take $x_0 \in S \cap (0,1)$ and set $K = \{p \in \mathbb{P} | \mathrm{v}_p(x_0) \neq 0\}$. Then K is finite. Let $p \in \mathbb{P} \setminus K$. Then $\mathbf{u}_0(S,p) \leq x_0 < 1$. Since $\mathbf{u}_0(S,p) \leq \mathbf{u}_0(S,p)\mathbf{u}_0(S,p)$ by 3.3.3, we have $\mathbf{u}_0(S,p) = 0$. If $\mathrm{v}_p(S) \neq \mathbb{Z}$ then, by 3.2.1 and 3.3.3, $\boldsymbol{u}(S,p) = \boldsymbol{e}_{(\infty,0)}$. If $\mathrm{v}_p(S) = \mathbb{Z}$ then, by 3.3.3, $\mathbf{u}_n(S,p) \leq \mathbf{u}_n(S,p)\mathbf{u}_0(S,p) = 0$ for every $n \in \mathbb{Z}$. □

Taking only the properties from 3.3.3 of a sequence (indexed by integers) we get, surprisingly, a quite good insight into the semiring S. That´s why we will more explore further properties of such sequences.

Definition 3.3.5. Denote $\overline{\mathfrak{R}}$ the set of all sequences $\boldsymbol{r} = (r_n)_{n\in\mathbb{Z}} \subseteq \bar{\mathbb{R}}_0^+$ such that

(i) $n \leq m \quad \Rightarrow \quad r_m \leq r_n$.

(ii) $r_{n+m} \leq r_n \cdot r_m$.

for all $n, m \in \mathbb{Z}$. The elements of $\overline{\mathfrak{R}}$ will be called *characteristic sequences.*

Further, let $\mathfrak{R}$ denotes the set of such sequences $\boldsymbol{r} = (r_n)_{n\in\mathbb{Z}} \in \overline{\mathfrak{R}}$ that $r_n < \infty$ for every $n \in \mathbb{Z}$.

Now we notice some properties of the characteristic sequences.

Lemma 3.3.6. *Let $\boldsymbol{r}, \boldsymbol{s} \in \overline{\mathfrak{R}}$.*

(i) If $r_{-1} < \infty$, then $\boldsymbol{r} \in \mathfrak{R}$.

(ii) Let $k \in \mathbb{N}_0$. Put $t_n = r_n$ for $n \geq k$ and $t_n = \infty$ for $n < k$. Then $\boldsymbol{t} = (t_n)_{n\in\mathbb{Z}} \in \overline{\mathfrak{R}}$. In particular, $\boldsymbol{e}_{(\infty,0)} \in \overline{\mathfrak{R}}$.

(iii) $\boldsymbol{r} \cdot \boldsymbol{s} \in \overline{\mathfrak{R}}$.

(iv) Let $\{\boldsymbol{t}_\alpha | \alpha \in I\} \subseteq \overline{\mathfrak{R}}$ be a family of characteristic sequences, then $\boldsymbol{t} = \sup\{\boldsymbol{t}_\alpha | \alpha \in I\} \in \overline{\mathfrak{R}}$.

Proof. (i) Clearly, $r_n \le r_{-1} < \infty$ for $n \in \mathbb{N}_0$ and, by the definition, $r_{-m} \le (r_{-1})^m < \infty$ for $m \in \mathbb{N}$.

(ii) and (iii). Easy.

(iv) Let $n, m \in \mathbb{N}$ and $t_k = \sup\{(t_\beta)_k | \beta \in I\}$ for $k \in \mathbb{Z}$. Then $(t_\alpha)_{n+m} \le (t_\alpha)_n (t_\alpha)_m \le t_n t_m$ for every $\alpha \in I$. Hence $t_{n+m} = \sup\{(t_\beta)_{n+m} | \beta \in I\} \le t_n t_m$. The rest is obvious. □

Lemma 3.3.7. *Let $\boldsymbol{r} \in \overline{\Re}$. Then either $\lim\limits_{n\to+\infty} r_n = 0$ or $r_n \ge 1$ for every $n \in \mathbb{N}_0$.*

Moreover, if $\boldsymbol{r} \in \Re$ then either $\boldsymbol{r} = 0$ or $r_{-n} \ge 1$ and $r_n > 0$ for every $n \in \mathbb{N}_0$.

Proof. First, assume that $r_k < 1$ for some $k \ge 0$. Since $\boldsymbol{r}$ is decreasing, we can suppose $k > 0$. Now, if $n \ge 2k$ then $n = lk + j$ for some $l \ge 2$ and $0 \le j < k$. We have $r_n \le r_{k+j} \cdot r_{(l-1)k} \le r_{k+j} \cdot r_k^{l-1}$. Therefore $r_n \le r_{k+j} \cdot r_k^{(n-j-k)/k}$ and it follows that $\lim\limits_{n\to+\infty} r_n = 0$.

Now, let $\boldsymbol{r} \in \Re$. If $r_{n_0} = 0$ for some $n_0 \in \mathbb{Z}$ then $0 \le r_n \le r_{n-n_0} r_{n_0} = 0$ for every $n \in \mathbb{Z}$. Suppose hence that $r_n \ne 0$ for every $n \in \mathbb{Z}$. Since $r_0 \le r_0 r_0$, it follows that $1 \le r_0 \le r_{-n}$ for every $n \in \mathbb{N}$. □

Following lemma records a very significant property of characteristic sequences, which will be later especially important in finding of all maximal subsemirings of $\mathbb{Q}^+$.

Lemma 3.3.8. *Let $k \in \mathbb{N}$ and $\{r_k, r_{k+1}, \dots\} \subseteq \mathbb{R}_0^+$ be a sequence such that $r_{n+m} \le r_n r_m$ for every $n, m \ge k$.*

Then $\lim\limits_{n\to+\infty} r_n^{1/n} = \inf\{r_n^{1/n} | n \ge k\}$.

Proof. Set $\lambda = \inf\{r_n^{1/n} | n \ge k\}$. Let $k \le m$ and $2m \le n$. Then $n = lm + j$ for some $l \ge 2$ and $0 \le j < m$. We have $r_n \le r_{m+j} \cdot r_{(l-1)m} \le r_{m+j} \cdot r_m^{l-1}$, and therefore $r_n^{1/n} \le r_{m+j}^{1/n} \cdot r_m^{(l-1)/n} = r_{m+j}^{1/n} \cdot (r_m^{1/m})^{(n-j-m)/n}$. Using this, one sees easily that $\limsup\limits_{n\to+\infty} r_n^{1/n} \le r_m^{1/m}$. Consequently, $\lambda \le \liminf\limits_{n\to+\infty} r_n^{1/n} \le \limsup\limits_{n\to+\infty} r_n^{1/n} \le \lambda$, and so $\lambda = \lim\limits_{n\to+\infty} r_n^{1/n}$. □

Definition 3.3.9. For $\boldsymbol{r} \in \overline{\Re}$ denote

$$\lambda^+(\boldsymbol{r}) = \inf\{r_n^{1/n} | n \ge 1\}$$

and

$$\lambda^-(\boldsymbol{r}) = \inf\{r_{-n}^{1/n} | n \ge 1\}.$$

Corollary 3.3.10. *Let $\boldsymbol{r} \in \overline{\Re}$. Then:*

(i) $\big(\lambda^+(\boldsymbol{r})\big)^n \leq r_n$ *and* $\big(\lambda^-(\boldsymbol{r})\big)^n \leq r_{-n}$ *for every* $n \in \mathbb{N}$.

(ii) $\lim\limits_{n \to +\infty} r_n^{1/n} = \lambda^+(\boldsymbol{r})$. *Moreover, if* $\boldsymbol{r} \neq \infty$ *then* $\lambda^+(\boldsymbol{r}) \leq 1$.

(iii) $\lim\limits_{n \to +\infty} r_{-n}^{1/n} = \lambda^-(\boldsymbol{r})$. *Moreover, if* $\boldsymbol{r} \neq 0$ *then* $\lambda^-(\boldsymbol{r}) \geq 1$.

(iv) $\lambda^+(\boldsymbol{r}) \cdot \lambda^-(\boldsymbol{r}) \geq 1$, *provided that* $\boldsymbol{r} \neq 0$.

(v) If $0 \neq \boldsymbol{r} \in \Re$ *then* $0 < \lambda^+(\boldsymbol{r}) \leq 1 \leq \lambda^-(\boldsymbol{r}) < \infty$. *Moreover, if* $r_n < 1$ *for at least one* $n \in \mathbb{N}$ *then* $0 < \lambda^+(\boldsymbol{r}) < 1 < \lambda^-(\boldsymbol{r}) < \infty$.

Proof. (i) Follows from 3.3.9.

(ii) Let $\boldsymbol{r} \neq \infty$. Then there is $n_0 \in \mathbb{N}$ such that $r_{n_0} < \infty$. Hence $r_n^{1/n} \leq r_{n_0}^{1/n}$ for every $n \geq n_0$ and $\inf\{r_n^{1/n} | n \geq n_0\} \leq \inf\{r_{n_0}^{1/n} | n \geq n_0\} = 1$. For the rest see 3.3.8.

(iii) If $r_{-1} = \infty$ then our assertion is clear. Now, if $r_{-1} < \infty$, then, by 3.3.6(i), $\boldsymbol{r} \in \Re$. Now use 3.3.7. For the rest see 3.3.8.

(iv) If $r_{-1} = \infty$ then $\lambda^+(\boldsymbol{r}) = \infty$ and $\lambda^+(\boldsymbol{r}) \cdot \lambda^-(\boldsymbol{r}) = \infty \geq 1$. Now, if $r_{-1} < \infty$ then $\boldsymbol{r} \in \Re$, by 3.3.6(i). Since $\boldsymbol{r} \neq 0$, we have $1 \leq r_0^{1/n} \leq r_n^{1/n} \cdot r_{-n}^{1/n}$ for every $n \geq 1$, by 3.3.7. Hence $1 \leq \lambda^+(\boldsymbol{r}) \cdot \lambda^-(\boldsymbol{r})$, by (ii) and (iii).

(v) For $0 \neq \boldsymbol{r} \in \Re$ use (ii),(iii) and (iv). If, in addition, $0 < r_{n_0} < 1$ for some $n_0 \in \mathbb{N}$ then $\lambda^+(\boldsymbol{r}) = \inf\{r_n^{1/n} | n \geq 1\} \leq r_{n_0}^{1/n_0} < 1$. Hence $\lambda^-(\boldsymbol{r}) > 1$, by (iv). □

We have already assigned characteristic sequences to a semiring. But, on the other hand, a semiring can be assigned to a characteristic sequence in a very natural way (see 3.3.11 and 3.3.13).

Definition 3.3.11. For $p \in \mathbb{P}$ and $\boldsymbol{r} \in \overline{\Re}$ denote

$$\mathbb{V}(p, \boldsymbol{r}) = \{x \in \mathbb{Q}^+ | r_{\mathrm{v}_p(x)} \leq x\}.$$

We will also often need the following observation concerning density.

Lemma 3.3.12. *Let* $m \in \mathbb{N}$, $p_1, p_2, \dots, p_m \in \mathbb{P}$ *be pair-wise different prime numbers and* $n_1, n_2, \dots, n_m \in \mathbb{Z}$.

Then $\{x \in \mathbb{Q}^* | \mathrm{v}_{p_i}(x) = n_i, 1 \leq i \leq m\}$ *is a dense subset of* $\mathbb{Q}$.

Proof. Let $r, s \in \mathbb{Q}$, $r < s$. Find $p_0 \in \mathbb{P} \setminus \{p_1, \dots, p_m\}$ such that $a = p_1^{n_1+1} \cdots p_m^{n_m+1}/p_0 < (s-r)/2$. Then $2a < s-r$ and $a = p_1 \cdots p_m b > b$, where $b = p_1^{n_1} \cdots p_m^{n_m}/p_0$. Obviously there is $k \in \mathbb{Z}$ such that $(k-1)a \leq r < ka$ and we put $t = ka + b = (kp_1 \cdots p_m + 1)b$. Clearly, $r < ka < t = (k-1)a + a + b \leq r + a + b < r + 2a < r + (s-r) = s$; thus $r < t < s$. Moreover, $\mathrm{v}_{p_i}(t) = \mathrm{v}_{p_i}((kp_1 \cdots p_m + 1)b) = \mathrm{v}_{p_i}(kp_1 \dots p_m + 1) + \mathrm{v}_{p_i}(b) = \mathrm{v}_{p_i}(b) = n_i$, for $1 \leq i \leq n$. □

In the next few statements we gather some knowledge about the semirings $\mathbb{V}(p, \boldsymbol{r})$.

Proposition 3.3.13. *Let $p \in \mathbb{P}$ and $\infty \neq \boldsymbol{r} \in \overline{\Re}$. Then:*

(i) $\mathbb{V}(p, \boldsymbol{r})$ *is a subsemiring of* $\mathbb{Q}^+$.

(ii) $\boldsymbol{u}(\mathbb{V}(p, \boldsymbol{r}), p) = \boldsymbol{r}$.

(iii) $\boldsymbol{u}(\mathbb{V}(p, \boldsymbol{r}), q) = \inf \boldsymbol{r}$ *for* $p \neq q \in \mathbb{P}$.

(iv) $\mathbb{V}(p, \boldsymbol{r})$ *is unitary if and only if* $r_0 \in \{0, 1\}$.

(v) $\mathbb{V}(p, \boldsymbol{r}) \cap (0, 1) \neq \emptyset$ *if and only if* $\inf \boldsymbol{r} = 0$.

(vi) $\mathtt{p}(\mathbb{V}(p, \boldsymbol{r})) \supseteq \mathbb{P} \setminus \{p\}$. *Moreover,* $p \in \mathtt{p}(\mathbb{V}(p, \boldsymbol{r}))$ *if and only if* $\boldsymbol{r} \in \Re$.

(vii) $\mathtt{pd}(\mathbb{V}(p, \boldsymbol{r})) \subseteq \{p\}$. *Moreover,* $\mathtt{pd}(\mathbb{V}(p, \boldsymbol{r})) = \{p\}$ *if and only if* $\inf \boldsymbol{r} = 0$ *and* $r_0 \geq 1$.

Proof. Set $V = \mathbb{V}(p, \boldsymbol{r})$.

(i) First, we show that $V \neq \emptyset$. Since $\boldsymbol{r} \neq \infty$, there is $n_0 \in \mathbb{N}$ such that $r_{n_0} < \infty$. By 3.3.12, there is $x \in \mathbb{Q}^+$ such that $r_{n_0} < x$ and $\mathrm{v}_p(x) = n_0$. Hence $x \in V$.

Now, we prove that V is closed under addition and multiplication. Let $a, b \in V$. Suppose, without loss of generality, that $\mathrm{v}_p(a) = \min\{\mathrm{v}_p(a), \mathrm{v}_p(b)\} \leq \mathrm{v}_p(a+b)$. Hence $r_{\mathrm{v}_p(a+b)} \leq r_{\mathrm{v}_p(a)} \leq a \leq a + b$ and $a + b \in V$. Further, $r_{\mathrm{v}_p(ab)} = r_{\mathrm{v}_p(a)+\mathrm{v}_p(b)} \leq r_{\mathrm{v}_p(a)} \cdot r_{\mathrm{v}_p(b)} \leq ab$. Thus $ab \in V$.

(ii) Let $n \in \mathbb{Z}$. Suppose first that $r_n = \infty$. Then, by 3.3.11, $n \notin \mathrm{v}_p(V)$. Hence $\mathbf{u}_n(V, p) = \infty$. Let be now $r_n < \infty$. Take $x \in V$ such that $\mathrm{v}_p(x) \leq n$. Then $r_n \leq r_{\mathrm{v}_p(x)} \leq x$. Hence $r_n \leq \inf\{x \in V | \mathrm{v}_p(x) \leq n\} = \mathbf{u}_n(V, p)$. Finally, by 3.3.12, for every $\varepsilon \in \mathbb{R}^+$ there is $x_0 \in \mathbb{Q}^+$ such that $r_n < x_0 < r_n + \varepsilon$ and $\mathrm{v}_p(x_0) = n$. Hence $r_n = \mathbf{u}_n(V, p)$.

(iii) Put $c = \inf \boldsymbol{r}$. Let $n \in \mathbb{Z}$ and q be a prime number different from p. Clearly, $c \leq \inf V$. Hence $c \leq \mathbf{u}_n(V, q)$. For every $\varepsilon \in \mathbb{R}^+$ there is $m \in \mathbb{Z}$ such that $c \leq r_m < c + \varepsilon$. Now again, by 3.3.12, there is $x_0 \in \mathbb{Q}^+$ such that $c \leq r_m < x_0 < c + \varepsilon$, $\mathrm{v}_p(x_0) = m$ and $\mathrm{v}_q(x_0) = n$. Hence $x_0 \in V$ and $c \leq \mathbf{u}_n(V, q) < c + \varepsilon$ for every $\varepsilon \in \mathbb{R}^+$. Thus $c = \mathbf{u}_n(V, q)$.

(iv) Clearly, V is unitary if and only if $r_0 \leq 1$. Since $r_0 \leq r_0 r_0$, we get that this is equivalent to $r_0 \in \{0, 1\}$.

(v) By (iv), $\inf \boldsymbol{r} = \inf V$. The rest now follows easily by 3.3.7.

(vi) Follows immediately from (ii) and (iii).

(vii) If $\inf \boldsymbol{r} > 0$ then, by (v), $\mathtt{pd}(V) = \emptyset$. Suppose now that $\inf \boldsymbol{r} = 0$. By (iii), $\boldsymbol{u}(V, q) = 0$ for every $q \in \mathbb{P}$ different from p. Hence $q \notin \mathtt{pd}(V)$ for any $q \neq p$. Finally, $p \in \mathtt{pd}(V)$ if and only if $r_0 \geq 1$. □

Remark 3.3.14. Let $p \in \mathbb{P}$ and $\boldsymbol{r} \in \overline{\Re}$. Then:

(i) $\mathbb{V}(p, \boldsymbol{r}) = \emptyset$ if and only if $\boldsymbol{r} = \infty$. (Use 3.3.13.)

(ii) $\mathbb{V}(p, \boldsymbol{r}) = \mathbb{Q}^+$ if and only if $\boldsymbol{r} = 0$. (Use 3.3.13(ii) and 3.3.12.)

(iii) Let $\{\boldsymbol{r}_\alpha | \alpha \in I\} \subseteq \overline{\Re}$ be a family of characteristic sequences. Then $\bigcap\limits_{\alpha \in I} \mathbb{V}(p, \boldsymbol{r}_\alpha) = \mathbb{V}(p, \boldsymbol{s})$, where $\boldsymbol{s} = \sup\{\boldsymbol{r}_\alpha | \alpha \in I\}$.

Proposition 3.3.15. *Let $p, q \in \mathbb{P}$ and $\boldsymbol{r}, \boldsymbol{s} \in \overline{\Re}$. Then $\mathbb{V}(p, \boldsymbol{r}) \subseteq \mathbb{V}(q, \boldsymbol{s})$ if and only if at least one of the following four conditions holds:*

(i) $\boldsymbol{s} = 0$.

(ii) $\boldsymbol{r} = \infty$.

(iii) $p = q$ *and* $\boldsymbol{s} \leq \boldsymbol{r}$.

(iv) $p \neq q$ *and* $\sup \boldsymbol{s} \leq \inf \boldsymbol{r}$.

Proof. If one of the conditions (i), (ii) or (iii) holds, our assertion is clearly true. Suppose the condition (iv). Let $x \in \mathbb{V}(p, \boldsymbol{r})$ and $\mathrm{v}_p(x) = n$. Then $s_{\mathrm{v}_q(x)} \leq \sup \boldsymbol{s} \leq \inf \boldsymbol{r} \leq r_n \leq x$. Hence $x \in \mathbb{V}(q, \boldsymbol{s})$.

The reverse implication follows from 3.3.13(ii),(iii) and 3.3.2. □

To see that also the case (iv) in previous proposition can occur, look at the next example.

Example 3.3.16. Let $a \in \mathbb{R}^+$, $1 \leq a$. If $\boldsymbol{r} = (r_n)_{n \in \mathbb{Z}} \subseteq \mathbb{R}^+$ is a descending sequence such that $a \leq \inf \boldsymbol{r} \leq \sup \boldsymbol{r} \leq a^2$, then $\boldsymbol{r} \in \Re$.

Remark 3.3.17. It follows easily from 3.3.15 that the subsemirings $\mathbb{V}(p, \boldsymbol{r})$ are pair-wise different for different pairs $(p, \boldsymbol{r})$, where $p \in \mathbb{P}$ and $\boldsymbol{r} \in \overline{\Re}$, $\boldsymbol{r}$ not constant. Due to 3.1.4, they are pair-wise non-isomorphic as well.

Notice that if $\boldsymbol{r} = r \in \overline{\Re}$ is constant, then $r = 0$ or $r \geq 1$ and $\mathbb{V}(p, \boldsymbol{r}) = \{x \in \mathbb{Q}^+ | r \leq x\}$.

3.4 Maximal subsemirings of $\mathbb{Q}^+$

It is quite easy to show that for $p \in \mathbb{P}$ is $\mathbb{U}_p = \{x \in \mathbb{Q}^* | \mathrm{v}_p(x) \geq 0\} \cup \{0\}$ a maximal subring of $\mathbb{Q}$ and that every proper subring of $\mathbb{Q}$ is contained in at least one of such rings. According to 3.1.1, these subrings are maximal as subsemirings as well. Further, it follows that if S is a proper subsemiring of $\mathbb{Q}$ such that $S \nsubseteq \mathbb{Q}_0^+$, then S is a subring by 3.1.1, and hence $S \subseteq \mathbb{U}(p)$ for a prime $p \in \mathbb{P}$.

We conclude easily that the subsemiring $\mathbb{Q}_0^+$ and the sub(semi)rings $\mathbb{U}_p$, $p \in \mathbb{P}$, are just all maximal subsemirings of $\mathbb{Q}$ and every proper subsemiring of $\mathbb{Q}$ is contained in one of them.

Now, we will look for maximal subsemirings of $\mathbb{Q}^+$.

Definition 3.4.1. Denote

$$\mathbb{Q}_1^+ = \{x \in \mathbb{Q}^+ | 1 \leq x\}.$$

Proposition 3.4.2. *$\mathbb{Q}_1^+$ is a (proper, unitary) maximal subsemiring of $\mathbb{Q}^+$. Further:*

(i) $\mathbb{Q}_1^+ = \mathbb{V}(p, \boldsymbol{r})$ *for any* $p \in \mathbb{P}$ *and* $\boldsymbol{r} = 1$.

(ii) $\boldsymbol{u}(\mathbb{Q}_1^+, p) = 1$ *for every* $p \in \mathbb{P}$.

(iii) $\mathtt{p}(\mathbb{Q}_1^+) = \mathbb{P}$.

(iv) $\mathtt{pd}(\mathbb{Q}_1^+) = \emptyset$.

(v) The difference ring $\mathbb{Q}_1^+ - \mathbb{Q}_1^+$ *is the field* $\mathbb{Q}$.

Proof. We show that $\mathbb{Q}_1^+$ is maximal. Take $a \in \mathbb{Q}^+ \cap (0,1)$. Let $x \in \mathbb{Q}^+ \cap (0,1)$. Then there is $n \in \mathbb{N}$ such that $y = x(a^{-1})^n \geq 1$. Hence $x \in \mathbb{Q}_1^+$ and $x = ya^n \in \left\langle \mathbb{Q}_1^+ \cup \{a\} \right\rangle$ and therefore $\left\langle \mathbb{Q}_1^+ \cup \{a\} \right\rangle = \mathbb{Q}^+$.

The rest is easy and follows from 3.3.13. □

Definition 3.4.3. For $p \in \mathbb{P}$ denote

$$\mathbb{S}_p = \{x \in \mathbb{Q}^+ | \mathrm{v}_p(x) \geq 0\}.$$

Proposition 3.4.4. *Let $p \in \mathbb{P}$. Then $\mathbb{S}_p$ is a (proper, unitary) maximal subsemiring of $\mathbb{Q}^+$. Further:*

(i) $\mathbb{S}_p = \mathbb{Q}^+ \cap \mathbb{U}_p = \mathbb{V}(p, \boldsymbol{r})$*, where* $\boldsymbol{r} = \boldsymbol{e}_{(\infty,0)}$*.*

(ii) $\boldsymbol{u}(\mathbb{S}_p, q) = 0$ *for every* $q \in \mathbb{P}$ *different from* p*.*

(iii) $\mathtt{p}(\mathbb{S}_p) = \mathbb{P} \setminus \{p\}$

(iv) $\mathtt{pd}(\mathbb{S}_p) = \emptyset$*.*

(v) The difference ring $\mathbb{S}_p - \mathbb{S}_p$ *is the ring* $\mathbb{U}_p$*.*

Proof. Clearly, $\mathbb{S}_p$ is a unitary subring of $\mathbb{Q}^+$. We show that it is maximal. Let $a \in \mathbb{Q}^+$ be such that $\mathrm{v}_p(a) < 0$. Then $a = b/p^k c$ for some $b, c, k \in \mathbb{N}$, where p does not divide b. We have $c/b \in \mathbb{S}_p$ and $1/p = p^{k-1} \cdot a \cdot c/b \in \langle \mathbb{S}_p \cup \{a\} \rangle$. Consequently, $\mathbb{Q}^+ = \langle \{1/q | q \in \mathbb{P}\} \rangle \subseteq \langle \mathbb{S}_p \cup \{a\} \rangle$. The remaining assertions are easy to check (use 3.3.13). □

Definition 3.4.5. For $p \in \mathbb{P}$ and $a \in (0,1) \subseteq \mathbb{R}$ put

$$\mathbb{W}(p, a) = \{x \in \mathbb{Q}^+ | a^{\mathrm{v}_p(x)} \leq x\}.$$

Proposition 3.4.6. *Let $p \in \mathbb{P}$ and $a \in (0,1)$. Then $\mathbb{W}(p, a)$ is a proper unitary subsemiring of $\mathbb{Q}^+$. Further:*

(i) $\mathbb{Q}_1^+ \cap \mathbb{S}_p \subseteq \mathbb{W}(p, a)$*.*

(ii) $\mathbb{W}(p, a) = \mathbb{V}(p, \boldsymbol{r})$*, where* $r_n = a^n$ *for every* $n \in \mathbb{Z}$*.*

(iii) $\boldsymbol{u}(\mathbb{W}(p, a), q) = 0$ *for every* $q \in \mathbb{P}$ *different from* p*.*

(iv) $\mathtt{p}(\mathbb{W}(p, a)) = \mathbb{P}$*.*

(v) $\mathtt{pd}(\mathbb{W}(p, a)) = \{p\}$*.*

(vi) The difference ring $\mathbb{W}(p, a) - \mathbb{W}(p, a)$ *is the field* $\mathbb{Q}$*.*

Proof. First, we show (vi). Denote $A = \mathbb{W}(p,a) - \mathbb{W}(p,a)$. Let $x \in \mathbb{Q}^+$ be such that $\mathrm{v}_p(x) < 0$. Take $p_1 \in \mathbb{P}$ such that $a^{\mathrm{v}_p(x)} < p_1$. Then $\mathrm{v}_p(p_1 + x) = \mathrm{v}_p(x)$ and $a^{\mathrm{v}_p(p_1+x)} = a^{\mathrm{v}_p(x)} < p_1 < p_1 + x$. Hence $p_1 + x \in \mathbb{W}(p,a)$. Of course, $p_1 \in \mathbb{W}(p,a)$, thus $x = (p_1 + x) - p_1 \in A$. Since $\mathrm{v}_p(1/qp) < 0$ for every $q \in \mathbb{P}$, we get that $1/q = p(1/qp) \in A$. Hence $\mathbb{Q}^+ \subseteq A$ and $A = \mathbb{Q}$.

The rest is easy. Use 3.3.13. □

To see that also the semirings $\mathbb{W}(p,a)$ are maximal in $\mathbb{Q}^+$ we will first need a few lemmas. In the end we show that the semirings mentioned above are indeed all maximal ones and every proper subsemiring of $\mathbb{Q}^+$ is contained in one of them.

Lemma 3.4.7. *Let $p, q \in \mathbb{P}$ and $a, b \in (0,1)$ be such that $\mathbb{W}(p,a) \subseteq \mathbb{W}(q,b)$. Then $p = q$ and $a = b$.*

Proof. By 3.4.6(ii) and 3.3.15, $p = q$ and $b^n \leq a^n$ for every $n \in \mathbb{Z}$. Hence $a = b$. □

Lemma 3.4.8. *Let S be a subsemiring of $\mathbb{Q}^+$. Then $S \subseteq \mathbb{V}(p, \boldsymbol{u}(S,p))$ for every $p \in \mathbb{P}$.*

Proof. Obvious. □

Lemma 3.4.9. *Let S be a subsemiring of $\mathbb{Q}^+$, $p \in \mathbb{P}$ and $a \in (0,1)$. Then:*

(i) $S \subseteq \mathbb{Q}_1^+$ if and only if $S \cap (0,1) = \emptyset$.

(ii) $\mathbb{P} \setminus \mathtt{p}(S) = \{p \in \mathbb{P} | S \subseteq \mathbb{S}_p\}$.

(iii) $S \subseteq \mathbb{W}(p,a)$ if and only if $a \leq \lambda^+(\boldsymbol{u}(S,p))$.

Proof. (i) and (ii). Obvious.

(iii) First, let $S \subseteq \mathbb{W}(p,a)$. By 3.3.2 and 3.3.13(ii), $a^n = \mathbf{u}_n(\mathbb{W}(p,a),p) \leq \mathbf{u}_n(S,p)$ for every $n \in \mathbb{Z}$. Hence $a \leq \lambda^+(\boldsymbol{u}(S,p))$, by 3.3.9.

Suppose now, on the other hand, that $0 < a \leq \lambda^+(\boldsymbol{r})$ for $\boldsymbol{r} = \boldsymbol{u}(S,p)$. Then $0 < a^n \leq r_n$ for every $n \in \mathbb{N}$. Hence, since $\boldsymbol{r}$ is decreasing and $r_0 \leq r_0^2$, we have $r_0 \neq 0$ and $1 \leq r_0$. If $r_{-1} = \infty$, then $a^{-n} \leq \infty = r_{-n}$ for every $n \in \mathbb{N}$.

Assume that $r_{-1} < \infty$. Then $\boldsymbol{r} \in \mathfrak{R}$, by 3.3.6(i). Since $\boldsymbol{r} \neq 0$, we get, by 3.3.10(iv),(v), that $\lambda^+(\boldsymbol{r})\lambda^-(\boldsymbol{r}) \geq 1$ and $\lambda^+(\boldsymbol{r}), \lambda^-(\boldsymbol{r}) \in \mathbb{R}^+$. Thus $a^{-n} \leq (\lambda^+(\boldsymbol{r}))^{-n} \leq (\lambda^-(\boldsymbol{r}))^n \leq r_{-n}$ for every $n \in \mathbb{N}$.

We conclude with $a^n \leq r_n$ for every $n \in \mathbb{Z}$. Hence $S \subseteq \mathbb{V}(p,\boldsymbol{r}) \subseteq \mathbb{W}(p,a)$, by 3.4.8 and 3.3.15(iii). □

Lemma 3.4.10. *Let S be a proper subsemiring of $\mathbb{Q}^+$ such that $S \not\subseteq \mathbb{Q}_1^+$ and $S \not\subseteq \mathbb{S}_p$ for every $p \in \mathbb{P}$. Then:*

(i) $\mathtt{p}(S) = \mathbb{P}$ *and* $\mathtt{pd}(S) \neq \emptyset$.

(ii) If $q \in \mathtt{pd}(S)$, *then* $a = \lambda^+(\boldsymbol{u}(S,q)) \in (0,1)$ *and* $S \subseteq \mathbb{W}(q,a)$.

Proof. (i) Clearly, if $q \in \mathbb{P} \setminus \mathtt{p}(S)$, then $S \subseteq \mathbb{S}_q$. Hence $\mathtt{p}(S) = \mathbb{P}$. Assume now that $\mathtt{pd}(S) = \emptyset$. By 3.2.7, $S = \left\langle \{\frac{1}{p} | p \in \mathtt{p}(S)\} \right\rangle$. Since $\mathtt{p}(S) = \mathbb{P}$, we get $S = \mathbb{Q}^+$, a contradiction.

(ii) By (i), $q \in \mathbb{P} = \mathtt{p}(S)$, hence $\boldsymbol{u}(S,q) \in \Re$. Since $q \in \mathtt{pd}(S)$, we have $\mathbf{u}_0(S,q) \geq 1$. Since $S \not\subseteq \mathbb{Q}_1^+$, there is $x_0 \in S \cap (0,1)$. Hence $\mathbf{u}_k(S,q) \leq x_0 < 1$ for $k = \mathrm{v}_q(x_0) \in \mathbb{Z}$ (in fact, $k \geq 1$ by the q-paradivisibility). Now, by 3.3.10(v), $a = \lambda^+(\boldsymbol{u}(S,q)) \in (0,1)$ and, by 3.4.9(iii), $S \subseteq \mathbb{W}(q,a)$. □

Proposition 3.4.11. *For all $p \in \mathbb{P}$ and $a \in (0,1)$, the subsemiring $\mathbb{W}(p,a)$ is maximal in $\mathbb{Q}^+$.*

Proof. Put $W = \mathbb{W}(p,a)$. By 3.4.6(iv),(v), we have $\mathtt{p}(W) = \mathbb{P}$ and $\mathtt{pd}(W) = \{p\}$. Consequently, $W \not\subseteq \mathbb{Q}_1^+$ and $W \not\subseteq \mathbb{S}_{p_1}$ for every $p_1 \in \mathbb{P}$. Now, let S be a proper subsemiring of $\mathbb{Q}^+$ such that $W \subseteq S$. By 3.4.10, $S \subseteq \mathbb{W}(p_2, b)$ for some $p_2 \in \mathtt{pd}(S)$ and $b \in (0,1)$. Thus $\mathbb{W}(p,a) \subseteq \mathbb{W}(p_2,b)$ and we get $p = p_2$ and $a = b$, by 3.4.7. Thus $\mathbb{W}(p,a)$ is a maximal subsemiring of $\mathbb{Q}^+$. □

Theorem 3.4.12. *The semirings $\mathbb{Q}_1^+$, $\mathbb{S}_p$ and $\mathbb{W}(p,a)$, $p \in \mathbb{P}$, $a \in (0,1)$ are just all (proper) maximal subsemirings of $\mathbb{Q}^+$. These subsemirings are pair-wise different (and hence non-isomorphic). Every proper subsemiring of $\mathbb{Q}^+$ is contained in (at least) one of them.*

Proof. By 3.4.2, 3.4.4 and 3.4.11, all the indicated subsemirings are maximal in $\mathbb{Q}^+$. If S is a maximal subsemiring of $\mathbb{Q}^+$ such that $S \neq \mathbb{Q}_1^+$ and $S \neq \mathbb{S}_p$ for every $p \in \mathbb{P}$, then, according to 3.4.10, we have $S = \mathbb{W}(q,a)$ for some $q \in \mathtt{pd}(S)$ and $a \in (0,1)$.

Comparing the characteristic sequences (see 3.4.2, 3.4.4 and 3.4.11) we get that all these subsemirings are pair-wise different, hence, by 3.1.4, pair-wise non-isomorphic.

The rest follows from 3.4.10. □

Remark 3.4.13. Note that all the maximal subsemirings of $\mathbb{Q}^+$ are unitary and of the form $\mathbb{V}(p, \boldsymbol{r})$ for suitable $p \in \mathbb{P}$ and $\boldsymbol{r} \in \overline{\Re}$ (see 3.4.2, 3.4.4 and 3.4.11).

Apart from 3.4.12, there is also a non-constructive way how to show, that every proper subsemiring of $\mathbb{Q}^+$ is contained in a maximal subsemiring of $\mathbb{Q}^+$. The next remark uses only Zorn's lemma and maximal subsemirings $\mathbb{Q}_1^+$ and $\mathbb{S}_p$, $p \in \mathbb{P}$.

Remark 3.4.14. Every proper subsemiring of $\mathbb{Q}^+$ is contained in a maximal subsemiring of $\mathbb{Q}^+$.

Indeed, let S be a proper subsemiring of $\mathbb{Q}^+$. If $S \cap (0,1) = \emptyset$, then $S \subseteq \mathbb{Q}_1^+$ and our result is true. Henceforth, we can assume that $S \cap (0,1) \neq \emptyset$. If $\mathtt{p}(S) \neq \mathbb{P}$, then $S \subseteq \mathbb{S}_p$ for $p \in \mathbb{P} \setminus \mathtt{p}(S)$. Thus suppose $\mathtt{p}(S) = \mathbb{P}$. Since S is a proper subsemiring of $\mathbb{Q}^+$, we have $\mathtt{pd}(S) \neq \emptyset$ by 3.2.7.

Let $\mathcal{T}$ denote the set of proper subsemirings T of $\mathbb{Q}^+$ such that $S \subseteq T$. Then $S \in \mathcal{T}$ and the set $\mathcal{T}$ is ordered by inclusion. Since $S \subseteq T$, we have $\mathbb{P} = \mathtt{p}(S) \subseteq \mathtt{p}(T)$, and so $\mathtt{p}(T) = \mathbb{P}$. Now, again, $\mathtt{pd}(T) \neq \emptyset$ follows from 3.2.7. Taking into account that $\mathrm{v}_p(1/2) \leq 0$ for all primes $p \in \mathbb{P}$, we conclude that $1/2 \notin T$ for every $T \in \mathcal{T}$. Consequently, the ordered set $\mathcal{T}$ is upwards inductive and it contains at least one maximal subsemiring.

Proposition 3.4.15. $\bigcap\limits_{p \in \mathbb{P}} \mathbb{S}_p = \mathbb{Q}_1^+ \cap \bigcap\limits_{p \in \mathbb{P}} \mathbb{S}_p = \mathbb{N}$.

Proof. It is obvious. □

Proposition 3.4.16. *Let S be a subsemiring of $\mathbb{Q}^+$. Then $S = \bigcap\limits_{p \in P} \mathbb{S}_p$ for a subset $P \subseteq \mathbb{P}$ if and only if either S is unitary and $\mathtt{p}(S) = \emptyset$ or $1/m \in S$ for some $2 \leq m \in \mathbb{N}$.*

Proof. ($\Rightarrow$) If $P = \mathbb{P}$ then $S = \mathbb{N}$, by 3.4.15. If $p \in \mathbb{P} \setminus P$ then $1/p \in S$.

($\Leftarrow$) If S is unitary and $\mathtt{p}(S) = \emptyset$, then $S = \mathbb{N}$ and we can set $P = \mathbb{P}$ (see 3.4.15). If $1/m \in S$ and $m \geq 2$, then $S \cap (0,1) \neq \emptyset$ and $\mathtt{pd}(S) = \emptyset$. Hence, by 3.2.7, $S = \left\langle \{\frac{1}{p} | p \in \mathtt{p}(S)\} \right\rangle = \bigcap\limits_{p \in \mathbb{P} \setminus \mathtt{p}(S)} \mathbb{S}_p$. □

Apart from the maximal-property of the set of all subsemirings in $\mathbb{Q}^+$, there holds another interesting statement namely, that taking a subsemiring S of $\mathbb{R}^+$ and having an "initial part" of a semiring (i.e., a set $M \subseteq S \cap (0,1)$ that fulfills the condition (i) and (ii) in 3.4.17), we have not only the least semiring $T \subseteq S$ such that $T \cap (0,1) = M$, but also the greatest one with this property (see 3.4.17).

Proposition 3.4.17. *Let and $M \subseteq S \cap (0,1)$ be a subset such that* *(i)* $(\forall\, x, x' \in M)(xx' \in M)$.

(ii) $(\forall\, x, x' \in M)(x + x' < 1 \Rightarrow x + x' \in M)$.

Denote $\overline{M} = \{y \in S \cap \langle 1, +\infty)|(\forall\, x \in M)(xy < 1 \Rightarrow xy \in M)\}$.

Then $S(M) = M \cup \overline{M}$ *is a unitary semiring and it is the greatest element of the set* $\{T \subseteq S | T \text{ is a semiring, } T \cap (0, 1) = M\}$.

Proof. First, we show that $S(M)$ is closed under multiplication.

For $x, x' \in M$ is $xx' \in M$ by assumption.

Let $x \in M$ and $y \in \overline{M}$. If $xy < 1$, then $xy \in M$. Suppose $xy \geq 1$. We show that $xy \in \overline{M}$. If $x' \in M$ is such that $x'(xy) < 1$, then $x'(xy) = (x'x)y \in M$, since $xx' \in M$ and $y \in \overline{M}$.

Let $y, y' \in \overline{M}$. We show that $yy' \in \overline{M}$. Let $x \in M$ be such that $x(yy') < 1$. Then $xy < 1$, since $y' \geq 1$. Therefore $xy \in M$ and thus $x(yy') = (xy)y' \in M$, since $y' \in \overline{M}$.

Further, we prove that $S(M)$ is closed under multiplication.

Let $a, b \in S(M)$. If $a + b < 1$ then $a, b < 1$. Hence $a, b \in M$ and therefore $a + b \in M$.

Suppose $a + b \geq 1$. Then we need to show, that $a + b \in \overline{M}$. Let $x \in M$ be such that $x(a + b) < 1$. Then $xa < 1$ and $xb < 1$. Since $S(M)$ is closed under multiplication, we have $xa, xb \in S(M)$ and it follows that $a' = xa \in M$, $b' = xb \in M$. Now, since $a' + b' < 1$, we get $x(a + b) = a' + b' \in M$. We have shown that $a + b \in \overline{M}$.

The rest is obvious. □

Chapter 4

Congruence-simple subsemirings of rational numbers

4.1 Introduction

In this chapter we will use the notation and results from the previous part. Let S be a semiring. A non-empty subset I of S is an *ideal* of S if $SI \subseteq I$ and $I + I \subseteq I$. A non-empty subset I of S is a *bi-ideal* of S if $SI \subseteq I$ and $S + I \subseteq I$.

A semiring S is said to be

(1) *congruence-simple* if it possess just two congruences.

(2) *ideal-simple* if S is non-trivial and it is the only ideal containing at least two elements.

(3) *bi-ideal-simple* if S is non-trivial and it is the only bi-ideal containing at least two elements.

Commutative congruence-simple semirings were characterized in [2, 10.1]. They are divided into several categories:

- There are just five non-isomorphic two-element semirings.
- The additively idempotent semirings $V(G)$:

  Let $G(\cdot)$ be an abelian group, $o \notin G$. Put $V(G) = G \cup \{o\}$ and define $x + y = y + x = o$, $x + x = x$ and $xo = ox = o$ for all $x, y \in V(G), x \neq y$.

- The additively idempotent and multiplicatively cancellative semirings $W(A)$:

  Let A be a non-zero subsemigroup of $\mathbb{R}(+)$ such that $A \cap \mathbb{R}^+ \neq \emptyset \neq A \cap \mathbb{R}^-$. Denote $W(A) = W(\oplus, \odot)$ the following semiring: $W(A) = A$, $a \oplus b = b \oplus a = \min\{a, b\}$ and $a \odot b = b \odot a = a + b$ for all $a, b \in A$.

- Fields.

- Zero-multiplication rings of finite prime order.

- (Congruence-simple) subsemirings of the semiring $\mathbb{R}^+$ of positive real numbers.

As we see from this list, only the subsemirings of $\mathbb{R}^+$ are not classified up to isomorphism yet. They are characterized though (see 4.1.1 and 4.1.2), but no explicit form of all of them is known. In this chapter we focus on the case of subsemirings of $\mathbb{Q}^+$.

Following assertions simplify the characterization of them.

Theorem 4.1.1. [2, 8.2] *Let S be a non-trivial semiring that is additively and multiplicatively cancellative. Then S is congruence-simple if and only if the following three conditions are satisfied:*

(i) S is archimedean: for all $a, b \in S$ there exist $c \in S$ and $n \in \mathbb{N}$ such that $b + c = na$.

(ii) S is conical: for all $a, b, c, d \in S$, $a \neq b$, there exist $e, f \in S$ such that $ae + bf + c = af + be + d$.

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

Lemma 4.1.2. [2, 9.1] *A subsemiring S of $\mathbb{Q}^+$ is archimedean and conical if and only if for every $n \in \mathbb{N}$ there exists $m \in \mathbb{N}$ such that $k/n \in S$ for every $k \geq m$.*

Theorem 4.1.3. [2, 9.5] *Let S be a congruence-simple subsemiring of $\mathbb{Q}^+$ such that $1 \in S$. Then $S = \mathbb{Q}^+$.*

Hence every proper congruence-simple subsemiring of positive rationals has to be non-unitary.

Remind also that, due 3.1.4, different subsemirings of $\mathbb{Q}^+$ are non-isomorphic. Hence the classification of the congruence-simple ones means to find all particular examples of them.

So far, only certain congruence-simple subsemirings of $\mathbb{Q}^+$ were found (see [13]), namely

$$\mathbb{T}_p(a) = \{x \in \mathbb{Q}^+ | a^{\mathrm{v}_p(x)} < x\}$$

where $p \in \mathbb{P}$ and $a \in (0,1)$, and their finite intersections.

Inspired by the machinery of the previous chapter we present a much bigger class of them.

4.2 A new class

Definition 4.2.1. Denote $\Re^\circ = \{\boldsymbol{r} = (r_n)_{n\in\mathbb{Z}} \in \Re | \lim_{n\to+\infty} r_n = 0\}$.

For $\boldsymbol{r} = (r_n)_{\in\mathbb{Z}} \in \overline{\Re}$ and $p \in \mathbb{P}$ set

$$\mathbb{V}^\circ(p, \boldsymbol{r}) = \{x \in \mathbb{Q}^+ | r_{\mathrm{v}_p(x)} < x\}.$$

Lemma 4.2.2. *Let $\infty \neq \boldsymbol{r} \in \overline{\Re}$ and $p \in \mathbb{P}$. Then $\mathbb{V}^\circ(p, \boldsymbol{r})$ is a semiring and $\boldsymbol{u}(\mathbb{V}^\circ(p, \boldsymbol{r}), p) = \boldsymbol{r}$.*

Proof. Set $V = \mathbb{V}^\circ(p, \boldsymbol{r})$. First, we show that $V \neq \emptyset$. Since $\boldsymbol{r} \neq \infty$, there is $n_0 \in \mathbb{N}$ such that $r_{n_0} < \infty$. By 3.3.12, there is $x \in \mathbb{Q}^+$ such that $r_{n_0} < x$ and $\mathrm{v}_p(x) = n_0$. Hence $x \in V$.

Now, we prove that V is closed under addition and multiplication. Let $a, b \in V$. Suppose, without loss of generality, that $\mathrm{v}_p(a) = \min\{\mathrm{v}_p(a), \mathrm{v}_p(b)\} \leq \mathrm{v}_p(a+b)$. Hence $r_{\mathrm{v}_p(a+b)} \leq r_{\mathrm{v}_p(a)} < a < a+b$ and $a+b \in V$. Further, $r_{\mathrm{v}_p(ab)} = r_{\mathrm{v}_p(a)+\mathrm{v}_p(b)} \leq r_{\mathrm{v}_p(a)} \cdot r_{\mathrm{v}_p(b)} < ab$. Thus $ab \in V$.

Finally, $V \subseteq \mathbb{V}(p, \boldsymbol{r})$. Hence, by 3.3.2 and 3.3.13(ii), we have $\boldsymbol{r} = \boldsymbol{u}(\mathbb{V}(p, \boldsymbol{r}), p) \leq \boldsymbol{u}(V, p)$. Let $n \in \mathbb{Z}$. We can assume, without loss of generality, that $r_n < \infty$. Now, by 3.3.12, for every $\varepsilon \in \mathbb{R}^+$ there is $x_0 \in \mathbb{Q}^+$ such that $r_n < x_0 < r_n + \varepsilon$ and $\mathrm{v}_p(x_0) = n$. Hence $r_n = \mathbf{u}_n(V, p)$. □

Comparing the previous lemma with 3.3.13(ii) we see that also $\mathbb{V}^\circ(p, \boldsymbol{r})$ has similar properties as $\mathbb{V}(p, \boldsymbol{r})$.

Lemma 4.2.3. *Let $p \in \mathbb{P}$ and $\boldsymbol{r}_1, \dots, \boldsymbol{r}_n \in \overline{\mathfrak{R}}$. Then $\bigcap\limits_{i=1}^{n} \mathbb{V}^\circ(p, \boldsymbol{r}_i) = \mathbb{V}^\circ(p, \boldsymbol{r})$, where $\boldsymbol{r} = \sup\{\boldsymbol{r}_i | i = 1, \dots, n\} \in \overline{\mathfrak{R}}$.*

Proof. Obvious. □

Now we introduce a new class of congruence-simple subsemirings of $\mathbb{Q}^+$.

Proposition 4.2.4. *Let $\boldsymbol{r}_1, \dots, \boldsymbol{r}_n \in \mathfrak{R}^\circ$ and $p_1, \dots, p_n \in \mathbb{P}$.*

Then $S = \bigcap\limits_{i=1}^{n} \mathbb{V}^\circ(p_i, \boldsymbol{r}_i)$ is a congruence-simple subsemiring of $\mathbb{Q}^+$.

Moreover, if $p_1, \dots, p_n$ are pair-wise different and $p \in \mathbb{P}$, then $\boldsymbol{u}(S, p) = \boldsymbol{r}_i$ if $p = p_i$, and $\boldsymbol{u}(S, p) = 0$ otherwise.

Proof. First, we show that $S \neq \emptyset$. In view of 4.2.3, we can assume, without loss of generality, that p_i are pair-wise different. Now, choose $k \in \mathbb{N}$. By 3.3.12, there is $x_0 \in \mathbb{Q}^+$ such that $\sup\{(r_i)_k | i = 1, \dots, n\} < x_0$ and $\mathrm{v}_{p_i}(x_0) = k$ for every $i = 1, \dots, n$. Hence $x_0 \in S$. By 4.2.2, S is a semiring.

Now, we prove that S is archimedean and conical. Let $m \in \mathbb{N}$. Take $k \in \mathbb{N}$ such that $k > \max\{m(r_i)_{-\mathrm{v}_{p_i}(m)} | i = 1, \dots, n\}$. Then for every $l \in \mathbb{N}$ such that $l \geq k$ we have $l/m \geq k/m > (r_i)_{-\mathrm{v}_{p_i}(m)} \geq (r_i)_{-\mathrm{v}_{p_i}(m)+\mathrm{v}_{p_i}(l)} = (r_i)_{\mathrm{v}_{p_i}(l/m)}$ for every $i = 1, \dots, n$. Hence $l/m \in S$. By 4.1.2, S is archimedean and conical.

Finally, we prove that S is bi-ideal-simple. According to 4.1.1, we have to show that for all $a, b \in S$ there exists $c \in S$ such that $a - bc \in S$.

So let $a, b \in S$. Set $s = \min\{a - (r_i)_{\mathrm{v}_{p_i}(a)} | i = 1, \dots, n\} > 0$. Since $\lim\limits_{k \to +\infty} (r_i)_k = 0$ for every i, there exists $k_0 \in \mathbb{N}$ such that $t = \max\{(r_i)_{k_0} | i = 1, \dots, n\} < s/b$ and $\max\{\mathrm{v}_{p_i}(a) - \mathrm{v}_{p_i}(b) | i = 1, \dots, n\} < k_0$.

By 3.3.12, there exists $c \in \mathbb{Q}^+$ such that $(r_i)_{k_0} \leq t < c < s/b$ and $\mathrm{v}_{p_i}(c) = k_0$ for every $i = 1, \dots, n$. Hence $c \in S$.

Now, $\mathrm{v}_{p_i}(c) = k_0 > \mathrm{v}_{p_i}(a) - \mathrm{v}_{p_i}(b)$, thus $\mathrm{v}_{p_i}(a) < \mathrm{v}_{p_i}(bc)$ and therefore $\mathrm{v}_{p_i}(a - bc) = \min\{\mathrm{v}_{p_i}(a), \mathrm{v}_{p_i}(-bc)\} = \mathrm{v}_{p_i}(a)$ for every $i = 1, \dots, n$. Hence $a - bc > a - s \geq (r_i)_{\mathrm{v}_{p_i}(a)} = (r_i)_{\mathrm{v}_{p_i}(a-bc)}$ and $a - bc \in S$. We have proved that S is bi-ideal-simple.

Thus, by 4.1.1, S is a congruence-simple semiring.

Finally, assume that $p_1, \dots, p_n$ are pair-wise different. Choose $i \in \{1, \dots, n\}$. Since $S \subseteq \mathbb{V}(p_i, \boldsymbol{r}_i)$, we get, by 3.3.2 and 3.3.13, that $\boldsymbol{r}_i \leq \boldsymbol{u}(S, p_i)$. Let $m \in \mathbb{Z}$. Since $\boldsymbol{r}_j \in \mathfrak{R}^\circ$ for every j, there is $k_0 \in \mathbb{N}$ such that $\max\{(r_j)_{k_0} | j = 1, \dots, n\} < (r_i)_n$. By 3.3.12, for every $\varepsilon \in \mathbb{R}^+$ there is $x_0 \in \mathbb{Q}^+$ such that $(r_j)_{k_0} < (r_i)_m < x_0 < (r_i)_m + \varepsilon$, $\mathrm{v}_{p_i}(x_0) = m$ and $\mathrm{v}_{p_j}(x_0) = k_0$ for every j such that $j \neq i$. Hence $x_0 \in S$ and it follows that $(r_i)_m = \mathbf{u}_m(V, p_i)$. We have proved that $\boldsymbol{r}_i = \boldsymbol{u}(S, p_i)$ for every $i = 1, \dots, n$.

Now, let $p \in \mathbb{P}$ be different from any p_i. Set $\boldsymbol{r} = 0$. Then $\mathbb{V}^\circ(p, \boldsymbol{r}) = \mathbb{Q}^+$. Hence $S' = S \cap \mathbb{V}^\circ(p, \boldsymbol{r}) = S$. Now, it easily follows that $0 = \boldsymbol{r} = \boldsymbol{u}(S', p) = \boldsymbol{u}(S, p)$. □

The next statements show that a general congruence-simple subsemiring of $\mathbb{Q}^+$ is very close to those that were already mentioned, namely there is a semiring from the new class that contains such particular semiring and, moreover, has the same characteristic sequences (see 4.2.6).

Proposition 4.2.5. *Let $S \subseteq \mathbb{Q}^+$ be a congruence-simple semiring. Then:*

(i) $S \cap (0, 1) \neq \emptyset$.

(ii) $\mathtt{p}(S) = \mathbb{P}$.

(iii) $\boldsymbol{u}(S, p) \in \Re^\circ$ *for every* $p \in \mathbb{P}$.

(iv) $(\forall x \in S)(\forall p \in \mathbb{P})(\mathbf{u}_{\mathrm{v}_p(x)}(S, p) < x)$.

Proof. (i) Suppose that $S \cap (0, 1) = \emptyset$. Take $a \in S$. By 4.1.1, S is bi-ideal-simple and we have $a = ac + d$ for some $c, d \in S$, where $a, c, d \geq 1$, a contradiction.

(ii) Let $p \in \mathbb{P}$. By 4.1.1, S is conical and archimedean and, by 4.1.2, there is $m \in \mathbb{N}$ such that $k/p \in S$ for every $k \geq m$. If $\gcd(k, p) = 1$ then, obviously, $v_p(k/p) = -1$. Hence $p \in \mathtt{p}(S)$, by 3.2.1.

(iii) Let $p \in \mathbb{P}$. Take $x_0 \in S \cap (0, 1)$. Set $n_0 = \mathrm{v}_p(x_0)$. Then $\mathbf{u}_{n_0}(S, p) \leq x_0 < 1$. By (ii), $\boldsymbol{u}(S, p) \in \Re$. Since $\boldsymbol{u}(S, p)$ is descending, we get, by 3.3.7, that $\lim\limits_{n \to +\infty} \mathbf{u}_n(S, p) = 0$.

(iv) Suppose, for contradiction, that $0 \neq a = \mathbf{u}_{\mathrm{v}_p(a)}(S, p)$ for some $a \in S$ and $p \in \mathbb{P}$. Hence, since $\boldsymbol{u}(S, p) \in \Re$, by (ii), we get, by 3.3.7, that $\mathbf{u}_0(S, p) \geq 1$.

By 4.1.1, S is bi-ideal-simple and hence there exists $c \in S$ such that $a - ac \in S$ and $c \neq 1$. Therefore $\mathbf{u}_{\mathrm{v}_p(a)}(S, p) = a > a - ac \geq \mathbf{u}_{\mathrm{v}_p(a-ac)}(S, p)$ and thus, by 3.3.3(i), $\mathrm{v}_p(a) + \mathrm{v}_p(1 - c) = \mathrm{v}_p(a - ac) > \mathrm{v}_p(a)$. Hence $\mathrm{v}_p(1 - c) > 0$ and therefore $\mathrm{v}_p(c) = 0$. Altogether, we have $c \geq \mathbf{u}_{\mathrm{v}_p(c)}(S, p) = \mathbf{u}_0(S, p) \geq 1$.

Now, $c \geq 1$ and it follows that $0 \geq a - ac \in S$, a contradiction. □

Corollary 4.2.6. *Let $S \subseteq \mathbb{Q}^+$ be a congruence-simple semiring.*

Put $K_S = \{p \in \mathbb{P} | \boldsymbol{u}(S, p) \neq 0\}$ *and* $T_S = \bigcap\limits_{p \in K_S} \mathbb{V}^\circ(p, \boldsymbol{u}(S, p))$. *Then:*

(i) K_S *is a finite set.*

(ii) T_S *is a congruence-simple semiring.*

(iii) $S \subseteq T_S$.

(iv) $\boldsymbol{u}(S,p) = \boldsymbol{u}(T_S,p)$ *for every* $p \in \mathbb{P}$.

Proof. (i) Follows from 3.3.4 and 4.2.5(ii).

(ii) Use 4.2.4 and 4.2.5.

(iii) Follows from 4.2.5(iv).

(iv) Follows from 4.2.4. □

Now we know that a finite intersection of the semirings of type $\mathbb{V}^\circ(p,\boldsymbol{r})$ is congruence-simple. We can ask whether this remains true for an arbitrary intersection. The next statement shows that in the case when such a semiring is congruence-simple, it must be a finite intersection of semirings of type $\mathbb{V}^\circ(p,\boldsymbol{r})$.

Proposition 4.2.7. *Let* I *be a set. Let* $\{\boldsymbol{r}_\alpha | \alpha \in I\} \subseteq \Re^\circ$ *be a family of characteristic sequences and* $\{p_\alpha | \alpha \in I\} \subseteq \mathbb{P}$ *be a family of primes.*

Let $S = \bigcap\limits_{\alpha\in I} \mathbb{V}^\circ(p_\alpha, \boldsymbol{r}_\alpha)$ *be a congruence-simple semirings. Then there are* $\boldsymbol{s}_1,\dots,\boldsymbol{s}_n \in \Re^\circ$ *and* $q_1,\dots,q_n \in \mathbb{P}$ *such that* $S = \bigcap\limits_{i=1}^{n} \mathbb{V}^\circ(q_i,\boldsymbol{s}_i)$.

Proof. We can assume, without loss of generality, that $I \neq \emptyset$ and $\boldsymbol{r}_\alpha \neq 0$ for every $\alpha \in I$.

We show that $\{p_\alpha | \alpha \in I\} \subseteq K_S$ (see 4.2.6). Suppose, on contrary, that there is $\alpha_0 \in I$ such that $p_{\alpha_0} \notin K_S$. Since $S \subseteq \mathbb{V}(p_{\alpha_0}, \boldsymbol{r}_{\alpha_0})$, we get, by 3.3.2 and 3.3.13(ii), that $0 \neq \boldsymbol{r}_{\alpha_0} \leq \boldsymbol{u}(S, p_{\alpha_0}) = 0$, a contradiction.

Now, there are $q_1,\dots,q_n \in \mathbb{P}$ such that $I_i = \{\alpha \in I | p_\alpha = q_i\} \neq \emptyset$ for every $i = 1,\dots,n$ and $I = \cup_{i=1}^n I_i$. Set $\boldsymbol{s}_i = \sup\{\boldsymbol{r}_\alpha | \alpha \in I_i\}$. By 3.3.14(iii), $S \subseteq \bigcap\limits_{\alpha\in I_i} \mathbb{V}(q_i, \boldsymbol{r}_\alpha) = \mathbb{V}(q_i,\boldsymbol{s}_i)$. Hence, by 3.3.2, 3.3.13(ii) and 4.2.5(iii), $\boldsymbol{s}_i \leq \boldsymbol{u}(S,q_i) \in \Re^\circ$. Thus, by 3.3.6(iv), $s_i \in \Re^\circ$.

Put $S_i = \bigcap\limits_{\alpha\in I_i} \mathbb{V}^\circ(q_i,\boldsymbol{r}_\alpha)$. Clearly, $\mathbb{V}^\circ(q_i,\boldsymbol{s}_i) \subseteq S_i$ and $S = \bigcap\limits_{j=1}^{n} S_j$. Hence $\bigcap\limits_{j=1}^{n} \mathbb{V}^\circ(q_j,\boldsymbol{s}_j) \subseteq S$ and thus, by 3.3.2 and 4.2.4, $\boldsymbol{u}(S,q_i) \leq \boldsymbol{s}_i$ for every $i = 1,\dots,n$. Therefore $\boldsymbol{u}(S,q_i) = \boldsymbol{s}_i$. Finally, by 4.2.6, $S \subseteq \bigcap\limits_{j=1}^{n} \mathbb{V}^\circ(q_j,\boldsymbol{u}(S,q_j)) = \bigcap\limits_{j=1}^{n} \mathbb{V}^\circ(q_j,\boldsymbol{s}_j)$. We conclude with $S = \bigcap\limits_{j=1}^{n} \mathbb{V}^\circ(q_j,\boldsymbol{s}_j)$. □

The following example shows that an infinite intersection of congruence-simple semirings needs not to be congruence-simple again.

Example 4.2.8. Remind that $\mathbb{T}_p(b) = \{x \in \mathbb{Q}^+ | b^{\mathrm{v}_p(x)} < x\}$ for $b \in (0,1)$ is a congruence-simple semiring.

Let $p \in \mathbb{P}$. Take $a \in \mathbb{Q}^+ \cap (0,1)$ such that $\mathrm{v}_p(a) = 1$ (such a exists by 3.3.12). Let $\{a_1, a_2, \dots\} \subseteq (0,1)$ be a sequence such that $a_1 < a_2 < \cdots$ and $\lim\limits_{n \to +\infty} a_n = a$. Consider $T = \bigcap\limits_{n=1}^{\infty} \mathbb{T}_p(a_n)$.

Then T is a semiring that is not congruence-simple, although it is an (infinite) intersection of congruence-simple semirings.

Indeed, $a_n^{\mathrm{v}_p(a)} = a_n < a$ for every $n \in \mathbb{N}$, hence $a \in T$ and $\mathbf{u}_1(T,p) \leq a$. Further, $T \subseteq \mathbb{T}_p(a_n)$, hence, by 3.3.2 and 4.2.4, $a_n = \mathbf{u}_1(\mathbb{T}_p(a_n),p) \leq \mathbf{u}_1(T,p)$ for every $n \in \mathbb{N}$. Thus $\mathbf{u}_{\mathrm{v}_p(a)}(T,p) = \mathbf{u}_1(T,p) = a$ and T is not congruence-simple, by 4.2.5(iv).

Finally, denote $\mathcal{C}ong\mathcal{S}imp = \{S \subsetneqq \mathbb{Q}^+ | S \textit{ is a congruence-simple semiring}\}$. We prove that this class has similar properties as the class of all proper subsemirings of $\mathbb{Q}^+$ (compare to 3.4.12).

Proposition 4.2.9. *The semirings $\mathbb{T}_p(a)$, where $p \in \mathbb{P}$, $a \in (0,1)$, are just all maximal elements of the set $\mathcal{C}ong\mathcal{S}imp$. These subsemirings are pair-wise different (and hence non-isomorphic). Every element of $\mathcal{C}ong\mathcal{S}imp$ is contained in (at least) one of them.*

Proof. Let $S \in \mathcal{C}ong\mathcal{S}imp$. By 4.2.5(i),(ii), $S \not\subseteq \mathbb{Q}_1^+$ and $S \not\subseteq \mathbb{S}_p$ for every $p \in \mathbb{P}$. Hence, by 3.4.12, there are $q \in \mathbb{P}$ and $a \in (0,1)$ such that $S \subseteq \mathbb{W}(q,a)$. Thus $a^n \leq \mathbf{u}_n(S,q)$ for every $n \in \mathbb{Z}$, by 3.3.2. Finally, $S \subseteq \mathbb{V}^\circ(q, \boldsymbol{u}(S,q)) \subseteq \mathbb{T}_q(a)$, by 4.2.6.

Comparing the characteristic sequences of $\mathbb{T}_p(a)$ (using 4.2.4), we obtain that all these semirings are pair-wise different.

The rest now follows easily. □

Chapter 5

Subparasemifields of $\mathbb{C}$

A (commutative) *parasemifield* is a semiring where the multiplicative part is a group. Clearly, a non-trivial parasemifield can not contain a zero element. The class of all parasemifield thus form a universal algebraic variety.

Let S be a parasemifield and let P denotes the smallest subparasemifield of S (i.e. the subparasemifield generated by 1_S (as a parasemifield)), then either P is trivial and S is additively idempotent or $P \cong \mathbb{Q}^+$ and S is not additively idempotent (see [15, 2.2]).

In [15] a conjecture was raised saying that every parasemifield that is finitely generated over $\mathbb{Q}^+$ as a semiring (i.e., is of the form $\mathbb{Q}^+[K]$ for some finite set K) is not finitely generated as a semiring. So far this is known for $|K| \leq 2$ (for $|K| \leq 1$ it was shown in [15] and the other result was not published yet).

In this section we will study the question when a semiring $\mathbb{Q}^+[\alpha] \subseteq \mathbb{C}$, $\alpha \in \mathbb{C}$, is a parasemifield. We find an equivalent condition under which is such a semiring contained in a parasemifield of $\mathbb{C}$. Moreover, we make a classification for the case when α is algebraic of degree 2 .

5.1 Preliminaries

First, we need to prove some auxiliary results.

For $n \in \mathbb{N}_0$ and $a, b, c, d \in \mathbb{R}$ set following polynomials

$$\mathbf{h}_n(c,d) = (x+1)\prod_{i=0}^{n}\left((x^2+d)^{2^i} + (cx)^{2^i}\right) \in \mathbb{R}[x]$$

$$\mathbf{g}_n(a,b,c,d) = (x^2+b-ax)\mathbf{h}_n(c,d) \in \mathbb{R}[x]$$

and

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

Lemma 5.1.1. $\mathbf{f}_n(a,b) = (x+1)\big((x^2+b)^{2^{n+1}} - (ax)^{2^{n+1}}\big)$ *and* $\mathbf{g}_n(a,b,c,d)$ *are monic polynomials of the same degree equal to* $2^{n+2}+1$ *for all* $a,b,c,d \in \mathbb{R}$.

Proof. Put $f = x^2+b$ and $g = ax$. We proceed by induction on $n \in \mathbb{N}_0$. For $n = 0$ we have $\mathbf{f}_0(a,b) = (f-g)(x+1)(f+g) = (x+1)(f^2-g^2)$.

Now, suppose $\mathbf{f}_n(a,b) = (x+1)(f^{2^{n+1}} - g^{2^{n+1}})$. Then $\mathbf{f}_{n+1}(a,b) = \mathbf{f}_n(a,b)(f^{2^{n+1}}+g^{2^{n+1}}) = (x+1)(f^{2^{n+1}}-g^{2^{n+1}})(f^{2^{n+1}}+g^{2^{n+1}}) = (x+1)(f^{2^{n+2}} - g^{2^{n+2}})$. The rest is obvious. □

Let $\mathbf{f}_n(a,b) = \sum_{k=0}^{2^{n+2}+1} r_k(n,a,b)x^k \in \mathbb{R}[x]$, where $r_k(n,a,b) \in \mathbb{R}$.

Lemma 5.1.2. *Let* $n \in \mathbb{N}_0$. *Assume that* $b > 0$ *and* $a \neq 0$. *Then the following conditions are equivalent:*

(i) $r_k(n,a,b) > 0$ *for every* $0 \le k \le 2^{n+2}+1$.

(ii) $\binom{2^{n+1}}{2^n}(b/a^2)^{2^n} > 1$.

Proof. By 5.1.1, we have $\mathbf{f}_n(a,b) = \big((x^2+b)^{2^{n+1}} - (ax)^{2^{n+1}}\big)(x+1) = \left(\sum_{i=0}^{2m}\binom{2m}{i}(x^{2i}+x^{2i+1})b^{2m-i}\right) - a^{2m}(x^{2m}+x^{2m+1})$, where $m = 2^n$.

Hence $r_k(n,a,b) > 0$ for every $0 \le k \le 2^{n+2}+1$ if and only if $\binom{2m}{m}b^m > a^{2m}$ with $m = 2^n$. □

Lemma 5.1.3. *Assume that* $4b > a^2 > 0$. *Then there are* $n_0 \in \mathbb{N}$ *and* $c,d \in \mathbb{Q}$ *such that* $(x^2+b-ax)\mathbf{h}_{n_0}(c,d) \in \mathbb{R}_0^+[x]$.

Proof. First, let $\mathbf{g}_n(a,b,u,v) = \sum_{k=0}^{2^{n+2}+1} s_k(n,a,b,u,v)x^k \in \mathbb{R}[x]$, where $s_k(n,a,b,u,v) \in \mathbb{R}$. Clearly, $s_k(n,a,b,\cdot,\cdot) : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ are polynomial functions and $s_k(n,a,b,a,b) = r_k(n,a,b)$ for every $a,b \in \mathbb{R}$, $n \in \mathbb{N}$ and $0 \le k \le 2^{n+2}+1$.

Now, put $r_m = \binom{2m}{m}(b/a^2)^m$ for $m \in \mathbb{N}$. Since $\lim_{m\to\infty}\frac{r_{m+1}}{r_m} = \lim_{m\to\infty}\frac{(2m+2)(2m+1)b}{(m+1)^2a^2} = \frac{4b}{a^2} > 1$, we have $\lim_{m\to\infty} r_m = \infty$. Hence, by 5.1.2, there are $n_0 \in \mathbb{N}$ and $\varepsilon \in \mathbb{R}^+$ such that $s_k(n_0,a,b,a,b) = r_k(n_0,a,b) > \varepsilon > 0$ for every

$0 \le k \le 2^{n_0+2}+1$. Since the functions $s_k(n_0, a, b, \cdot, \cdot)$ are continuous, there are $c, d \in \mathbb{Q}$ such that $s_k(n_0, a, b, c, d) > 0$ for every $0 \le k \le 2^{n_0+2}+1$. It follows that $(x^2+b-ax)\mathbf{h}_{n_0}(c, d) = \mathbf{g}_{n_0}(a, b, c, d) \in \mathbb{R}_0^+[x]$. □

Proposition 5.1.4. *Let F be a subfield of $\mathbb{R}$ and $0 \neq f \in F[x]$. The following conditions are equivalent:*

(i) There exists $0 \neq h \in \mathbb{Q}[x]$ such that $hf \in F_0^+[x]$.

(ii) The polynomial f has no positive real root (in $\mathbb{C}$).

Proof. (i)⇒(ii). Let $0 \neq g = hf \in F_0^+[x]$. Suppose, on contrary, that $f(a) = 0$ for some $a \in \mathbb{R}^+$. Then $0 < g(a) = h(a)f(a) = 0$, a contradiction.

(ii)⇒(i). We can assume f to be monic. Let $f = f_1 \cdots f_n$ be the decomposition of f into monic polynomials f_i that are irreducible in $\mathbb{R}[x]$. Clearly, $\deg(f_i) \in \{1, 2\}$ and no f_i has a positive real root.

Let $\deg(f_i) = 1$. Then $f_i = x+e$ for some $e \in \mathbb{R}_0^+$ and we set $h_i = 1 \in \mathbb{Q}[x]$. Now, let $\deg(f_i) = 2$. Then $f_i = x^2 - ax + b$, where $a, b \in \mathbb{R}$ and $a^2 - 4b < 0$. Thus $b > 0$. If $a \le 0$ we set, again, $h_i = 1 \in \mathbb{Q}[x]$. Now, if $a > 0$, then there is, by 5.1.3, $0 \neq h_i \in \mathbb{Q}[x]$ such that $h_i f_i \in \mathbb{R}_0^+[x]$.

For every $i = 1, \dots, n$ we have found $0 \neq h_i \in \mathbb{Q}[x]$ such that $h_i f_i \in \mathbb{R}_0^+[x]$. Now, we just set $h = h_1 \cdots h_n \in \mathbb{Q}[x]$. □

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

For $\alpha \in \mathbb{C}$ let $\mathbb{Q}^+[\alpha]$ denote the subsemiring of $\mathbb{C}$ generated by $\mathbb{Q}^+ \cup \{\alpha\}$. Clearly, $\mathbb{Q}^+[\alpha] = \{f(\alpha) | 0 \neq f \in \mathbb{Q}_0^+[x]\}$.

For $\alpha \in \mathbb{C}$ algebraic (over $\mathbb{Q}$) denote $\min_{\mathbb{Q}}(\alpha) \in \mathbb{Q}[x]$ the minimal monic polynomial in $\mathbb{Q}[x]$ with a root α.

Remark 5.2.1. (i) If $\alpha \in \mathbb{C}$ is transcendental, then $\mathbb{Q}^+[\alpha] \cong \mathbb{Q}^+[x]$.

(ii) Let $\alpha, \beta \in \mathbb{C}$ be algebraic numbers with the same minimal polynomial in $\mathbb{Q}[x]$. Then the mapping $f(\alpha) \mapsto f(\beta)$, $f \in \mathbb{Q}^+[x]$, is an isomorphism of the semiring $\mathbb{Q}^+[\alpha]$ onto the semiring $\mathbb{Q}^+[\beta]$.

Indeed, if $f_1(\alpha) = f_2(\alpha)$, then $\min_{\mathbb{Q}}(\alpha)$ divides the difference $f_1 - f_2$. But then $(f_1 - f_2)(\beta) = 0$, and hence $f_1(\beta) = f_2(\beta)$. The rest is clear.

Proposition 5.2.2. *Let $0 \neq \alpha \in \mathbb{C}$ be an algebraic number. The following conditions are equivalent:*

(i) $\mathbb{Q}^+[\alpha]$ *is a subfield of* $\mathbb{C}$.

(ii) $0 \in \mathbb{Q}^+[\alpha]$.

(iii) The minimal polynomial $\min_{\mathbb{Q}}(\alpha)$ *has no positive real roots.*

Proof. (ii)⇒(i). Put $A = \mathbb{Q}^+[\alpha] \cap \mathbb{Q}$. If $0 \in \mathbb{Q}^+[\alpha]$, then there are $n \in \mathbb{N}$ and $a_0, \dots, a_n \in \mathbb{Q}_0^+$ such that $0 = a_0 + a_1\alpha + \cdots + a_n\alpha^n$ and $a_n \neq 0$. Assume that n is the smallest possible. Then $a_0 > 0$ and $-a_0 = a_1\alpha + \cdots + a_n\alpha^n \in \mathbb{Q}^+[\alpha] \cap \mathbb{Q}^- \subseteq A$.

Now, A is a subsemiring of $\mathbb{Q}$, $\mathbb{Q}^+ \subseteq A$ and $A \cap \mathbb{Q}^- \neq \emptyset$. Consequently, $\mathbb{Q} = A \subseteq \mathbb{Q}^+[\alpha]$ and $\mathbb{Q}^+[\alpha] = \mathbb{Q}[\alpha]$ is a field.

(i)⇒(iii). Clearly, $0 \in \mathbb{Q}^+[\alpha]$. Hence there is $0 \neq g \in \mathbb{Q}_0^+[x]$ such that $g(\alpha) = 0$. Thus g is divisible by $f = \min_{\mathbb{Q}}(\alpha) \in \mathbb{Q}[x]$ and there is $0 \neq h \in \mathbb{Q}[x]$ such that $hf = g \in \mathbb{Q}_0^+[x]$. Now, by 5.1.4, f has no positive real root.

(iii)⇒(ii). Suppose $f = \min_{\mathbb{Q}}(\alpha) \in \mathbb{Q}[x]$ has no positive real root. By 5.1.4, there is $0 \neq h \in \mathbb{Q}[x]$ such that $0 \neq g = hf \in \mathbb{Q}_0^+[x]$. Hence $0 = g(\alpha) \in \mathbb{Q}^+[\alpha]$. □

Denote $\sqrt[\infty]{1} = \{z \in \mathbb{C} | (\exists n \in \mathbb{N})(z^n = 1)\}$ the subgroup of all element of finite order in $\mathbb{C}^*$.

Corollary 5.2.3. *Let* $\alpha \in \mathbb{C}$ *be an algebraic number.*

Then $\mathbb{Q}^+[\alpha]$ *is a field if and only if* $\sqrt[\infty]{1} \cap \mathbb{Q}^+[\alpha] \neq \{1\}$.

Proof. (⇒) If $\mathbb{Q}^+[\alpha]$ is a field, then $-1 \in \sqrt[\infty]{1} \cap \mathbb{Q}^+[\alpha]$.

(⇐) There is $1 \neq \beta \in \mathbb{Q}^+[\alpha]$, such that $\beta^m = 1$ for some $m \geq 2$. We have $\beta\gamma = \gamma$, where $\gamma = 1 + \beta + \cdots + \beta^{m-1} \in \mathbb{Q}^+[\alpha]$. Since $\beta \neq 1$, it follows that $\gamma = 0$, and hence $0 \in \mathbb{Q}^+[\alpha]$. It remains to use 5.2.2. □

The multiplicative group of a parasemifield needs always to be torsion-free (see [15, 2.8]). Comparing to the result in 5.2.3, we have that for a parasemifield $S \subseteq \mathbb{C}$ holds $\sqrt[\infty]{1} \cap S = \{1\}$.

Corollary 5.2.4. *Let* $\alpha \in \mathbb{C}$. *The following conditions are equivalent:*

(i) $\mathbb{Q}^+[\alpha]$ *is contained in a subparasemifield of* $\mathbb{C}$.

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

(iii) Either α *is transcendental or* $\alpha \neq 0$ *is algebraic and the minimal polynomial* $\min_{\mathbb{Q}}(\alpha)$ *has a positive real root.*

Proof. (i)$\Rightarrow$(ii). Obvious.

(ii)$\Rightarrow$(iii). Follows from 5.2.2.

(iii)$\Rightarrow$(i). If α is transcendental then $\mathbb{Q}^+[\alpha] \cong \mathbb{Q}^+[x]$ and thus it can not contain a zero-element. If $\alpha \neq 0$ is algebraic and the minimal polynomial $\min_{\mathbb{Q}}(\alpha)$ has a positive real root then, by 5.2.2, $0 \notin \mathbb{Q}^+[\alpha]$. In both cases $P = \{ab^{-1} | a, b \in \mathbb{Q}^+[\alpha]\} \subseteq \mathbb{C}$ is a parasemifield. □

Now, we have found a equivalent condition under which is the semiring $\mathbb{Q}^+[\alpha]$ contained in a subparasemifield of $\mathbb{C}$. However, this inclusion can happen to proper and such a semiring needs not to be a parasemifield. We will see it in the next classification of the case when α is algebraic of degree 2.

Remark 5.2.5. (i) Let $\alpha \in \mathbb{C}$ be algebraic of degree 2. Then the minimal polynomial $\min_{\mathbb{Q}}(\alpha)$ has a positive real root if and only if there exist $q \in \mathbb{Q}^+$ and $t \in \mathbb{Q}$ such that $-t < \sqrt{q} \notin \mathbb{Q}$ and either $\alpha = \sqrt{q} + t$ or $\alpha = -\sqrt{q} + t$.

(ii) Let $q \in \mathbb{Q}^+$ be such that $\sqrt{q} \notin \mathbb{Q}$. Denote $(a + b\sqrt{q})^* = a - b\sqrt{q}$ for $a, b \in \mathbb{Q}$. The map $\varphi : \mathbb{Q}[\sqrt{q}] \to \mathbb{Q}[\sqrt{q}]$, $\varphi(x) = x^*$ for $x \in \mathbb{Q}[\sqrt{q}]$, is the only non-trivial isomorphism of the field $\mathbb{Q}[\sqrt{q}]$ that is identical on $\mathbb{Q}$. Moreover, if $\beta \in \mathbb{Q}[\sqrt{q}]$ is algebraic of degree 2, then β^* is the associated root for β, i.e. $\min_{\mathbb{Q}}(\beta) = (x - \beta)(x - \beta^*)$.

(iii) Clearly, $P = \{x \in \mathbb{Q}[\sqrt{q}] | x > 0, x^* > 0\} = \{a + b\sqrt{q} | a, b \in \mathbb{Q}, a > |b|\sqrt{q}\}$ is a parasemifield. Moreover, $P = \mathbb{Q}[\sqrt{q}]^+ \cap \varphi(\mathbb{Q}[\sqrt{q}]^+)$ and $\varphi(P) = P$.

Lemma 5.2.6. *Let $a, b \in \mathbb{Q}^+$ and $\mathbb{Q}^+ \subseteq A \subseteq \mathbb{R}^+$ be a semiring. Then:*

(i) If $-\sqrt{q} + a, -\sqrt{q} + b \in A$, then $-\sqrt{q} + \frac{ab+q}{a+b} \in A$ and $\sqrt{q} < \frac{ab+q}{a+b} < a, b$.

(ii) If $\sqrt{q} - a, -\sqrt{q} + b \in A$, then $\sqrt{q} - \frac{ab+q}{a+b} \in A$ and $0 < a < \frac{ab+q}{a+b} < \sqrt{q} < b$.

Proof. (i) We have $-\sqrt{q} + \frac{ab+q}{a+b} = \frac{1}{a+b}(-\sqrt{q} + a)(-\sqrt{q} + b) \in A$. Since $A \subseteq \mathbb{R}^+$, $\sqrt{q} < \frac{ab+q}{a+b}$. Finally, $q < a^2$, hence $q + ab < a^2 + ab$ and $\frac{ab+q}{a+b} < a$. Similarly, $\frac{ab+q}{a+b} < b$.

(ii) We have $\sqrt{q} - \frac{ab+q}{a+b} = \frac{1}{a+b}(\sqrt{q} - a)(-\sqrt{q} + b) \in A$. Since $A \subseteq \mathbb{R}^+$, $\frac{ab+q}{a+b} < \sqrt{q}$. Finally, $a^2 < q$, hence $a^2 + ab < q + ab$ and $a < \frac{ab+q}{a+b}$. □

Lemma 5.2.7. *Let $\mathbb{Q}^+ \subseteq A \subseteq \mathbb{R}^+$ be a semiring.*

(i) If $-\sqrt{q} + r \in A$ for some $r \in \mathbb{Q}^+$, then $-\sqrt{q} + a \in A$ for every $a \in \mathbb{Q}^+$ such that $\sqrt{q} < a$.

(ii) If $\sqrt{q} - r \in A$ for some $r \in \mathbb{Q}^+$, then $\sqrt{q} - a \in A$ for every $a \in \mathbb{Q}^+$ such that $a < \sqrt{q}$.

Proof. (i) First, we find a descending sequence $(r_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q}^+$ such that $-\sqrt{q}+r_n \in A$ for every $n \in \mathbb{N}$ and $\lim\limits_{n\to\infty} r_n = \sqrt{q}$.

We proceed by induction. Put $r_1 = r$. Now, suppose that r_n is already defined. Put $r_{n+1} = \frac{r_n^2+q}{2r_n}$. Since $-\sqrt{q}+r_n \in A$, we have, by 5.2.6(i), that $\sqrt{q} < r_{n+1} < r_n$ and $-\sqrt{q}+r_{n+1} \in A$. Now, our sequence is descending and $\sqrt{q} < r_n$ for every $n \in \mathbb{N}$. Thus it has a limit $\lambda \in \mathbb{R}^+$ and we have $\lambda = \lim\limits_{n\to\infty} r_{n+1} = \lim\limits_{n\to\infty} \frac{r_n^2+q}{2r_n} = \frac{\lambda^2+q}{2\lambda}$. Hence $\lambda = \sqrt{q}$.

Finally, let $a \in \mathbb{Q}^+$ be such that $\sqrt{q} < a$. Then $r_{n_0} < a$ for some $n_0 \in \mathbb{N}$ and we have $a - r_{n_0} \in \mathbb{Q}^+$ and $-\sqrt{q}+a = (-\sqrt{q}+r_{n_0}) + (a - r_{n_0}) \in A$.

(ii) Put $s = \frac{r^2+q}{2r} \in \mathbb{Q}^+$. Then $-\sqrt{q}+s = -\sqrt{q}+\frac{r^2+q}{2r} = \frac{1}{2r}(\sqrt{q}-r)^2 \in A$.

We find, similarly, an ascending sequence $(s_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q}^+$ such that $\sqrt{q} - s_n \in A$ for every $n \in \mathbb{N}$ and $\lim\limits_{n\to\infty} s_n = \sqrt{q}$.

We proceed by induction. Put $s_1 = r$. Now, suppose that s_n is already defined. Put $s_{n+1} = \frac{s_n s+q}{s_n+s}$. Since $\sqrt{q} - s_n, -\sqrt{q}+s \in A$, we have, by 5.2.6(ii), that $s_n < s_{n+1} < \sqrt{q}$ and $\sqrt{q} - s_{n+1} \in A$. Now, our sequence is ascending and $s_n < \sqrt{q}$ for every $n \in \mathbb{N}$. Thus it has a limit $\mu \in \mathbb{R}^+$ and we have $\mu = \lim\limits_{n\to\infty} s_{n+1} = \lim\limits_{n\to\infty} \frac{s_n s+q}{s_n+s} = \frac{\mu s+q}{\mu+s}$. Hence $\mu = \sqrt{q}$.

Finally, if $a \in \mathbb{Q}^+$ is such that $a < \sqrt{q}$, then $a < s_{n_0}$ for some $n_0 \in \mathbb{N}$ and we have $s_{n_0} - a \in \mathbb{Q}^+$ and $\sqrt{q} - a = (\sqrt{q} - s_{n_0}) + (s_{n_0} - a) \in A$. □

Note that for a semiring $A \subseteq \mathbb{C}$ that does not contain 0, the set $AA^{-1} = \{ab^{-1} | a, b \in A\}$ is a parasemifield generated (as a parasemifield) by the set A.

Proposition 5.2.8. *Let $\alpha = \sqrt{q}+t$, where $q \in \mathbb{Q}^+$, $t \in \mathbb{Q}$ and $\sqrt{q} \notin \mathbb{Q}$. Put $A = \mathbb{Q}^+[\alpha]$. Then:*

(i) If $t < -\sqrt{q}$, then $A = \mathbb{Q}[\sqrt{q}]$ and $A^* = \mathbb{Q}[\sqrt{q}] \setminus \{0\}$.

(ii) If $-\sqrt{q} < t < 0$, then $A = A^* = AA^{-1} = \mathbb{Q}[\sqrt{q}]^+$.

(iii) If $t = 0$, then $A = \mathbb{Q}^+[\sqrt{q}]$, $A^* = \{a, a\sqrt{q} | a \in \mathbb{Q}^+\}$ and $AA^{-1} = \mathbb{Q}[\sqrt{q}]^+$.

(iv) If $0 < t < \sqrt{q}$, then $A \subsetneqq \mathbb{Q}^+[\sqrt{q}]$, $A^* = \mathbb{Q}^+$ and $AA^{-1} = \mathbb{Q}[\sqrt{q}]^+$.

(v) If $\sqrt{q} < t$, then $A \subsetneqq \mathbb{Q}^+[\sqrt{q}]$, $A^* = \mathbb{Q}^+$ and $AA^{-1} = \{a + b\sqrt{q} | a, b \in \mathbb{Q}, a > |b|\sqrt{q}\} \subsetneqq \mathbb{Q}[\sqrt{q}]^+$.

Proof. (i) By 5.2.5 and 5.2.2, $A = \mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{q}]$.

(ii) Clearly, $A \subseteq \mathbb{Q}[\sqrt{q}]^+$. We show that $\mathbb{Q}[\sqrt{q}]^+ = \{a + b\sqrt{q} > 0 | a, b \in \mathbb{Q}\} \subseteq A$. In particular, since $\mathbb{Q}^+ \subseteq A$, it is enough to prove that $\sqrt{q} - r \in A$ for every $r \in \mathbb{Q}$, $r < \sqrt{q}$, and that $-\sqrt{q} + s \in A$ for every $s \in \mathbb{Q}$, $\sqrt{q} < s$.

First, we have $\sqrt{q}+t = \alpha \in A$, where $t < 0$. Hence, by 5.2.7(ii), $\sqrt{q}-r \in A$ for every $r \in \mathbb{Q}$ such that $0 < r < \sqrt{q}$. If $0 \geq r \in \mathbb{Q}$, then $-t - r \in \mathbb{Q}^+$ and $\sqrt{q} - r = (\sqrt{q} + t) + (-r - t) \in A$.

Further, $-\sqrt{q} + \frac{t^2+q}{-2t} = \frac{1}{-2t}(\sqrt{q} + t)^2 \in A$. Since $\frac{t^2+q}{-2t} > 0$, we get, by 5.2.7(i), that $-\sqrt{q} + s \in A$ for every $s \in \mathbb{Q}$, $\sqrt{q} < s$.

We conclude with $\mathbb{Q}[\sqrt{q}]^+ = A$.

(iii) and (iv). Let $0 \leq t < \sqrt{q}$, then, clearly, $A \subseteq \mathbb{Q}^+[\sqrt{q}] = \{a+b\sqrt{q} | a, b \in \mathbb{Q}_0^+, a + b \neq 0\}$. Now, let $a + b\sqrt{q} \in A^*$, $a, b \in \mathbb{Q}^+$, $a + b \neq 0$. Of course, $a/c + (-b/c)\sqrt{q} = (a + b\sqrt{q})^{-1} \in \mathbb{Q}^+[\sqrt{q}]$, where $c = a^2 - b^2 q \neq 0$. Hence $b = 0$, if $c > 0$, and $a = 0$, if $c < 0$. The assertion for A^* now follows easily.

Finally, put $U = AA^{-1}$. Since $A \subseteq \mathbb{Q}^+[\sqrt{q}]$, we have $U \subseteq \mathbb{Q}^+[\sqrt{q}]$. Obviously, there is $r \in \mathbb{Q}$ such that $t < r < \sqrt{q}$ and $\sqrt{q} + r \in A$. Thus $\sqrt{q} - \frac{r}{q-r^2} = (q - r^2)(\sqrt{q} + r)^{-1} \in A^{-1} \subseteq U$. Hence, since $0 < \frac{r}{q-r^2} < \sqrt{q}$, we get, by (ii), that $\mathbb{Q}[\sqrt{q}]^+ = \mathbb{Q}^+[\sqrt{q} - \frac{r}{q-r^2}] \subseteq U$. Thus $\mathbb{Q}[\sqrt{q}]^+ = U$.

(v) Take $0 < t' < \sqrt{q}$, $t' \in \mathbb{Q}$. Clearly, by (iv), $\mathbb{Q}^+ \subseteq A^* \subseteq \mathbb{Q}^+[t']^* = \mathbb{Q}^+$ and $A^* = \mathbb{Q}^+$.

Now, by 5.2.5(iii), $P = \{a + b\sqrt{q} | a, b \in \mathbb{Q}, a > |b|\sqrt{q}\}$ is a parasemifield and $\mathbb{Q}^+ \cup \{\alpha\} \subseteq P$. Hence $A = \mathbb{Q}^+[\alpha] \subseteq P$ and $AA^{-1} \subseteq P$. Now, $-\sqrt{q} + t = (t^2 - q)(\sqrt{q} + t)^{-1} \in A^{-1} \subseteq AA^{-1}$, since $\sqrt{q} < t$. By 5.2.7(i), $-\sqrt{q} + c \in AA^{-1}$ for every $c \in \mathbb{Q}^+$ such that $\sqrt{q} < c$. Hence $\sqrt{q}+c = (c^2-q)(-\sqrt{q}+c)^{-1} \in AA^{-1}$ for every $c \in \mathbb{Q}^+$ such that $\sqrt{q} < c$. Now, easily follows that $\{a + b\sqrt{q} | a, b \in \mathbb{Q}, a > |b|\sqrt{q}\} \subseteq AA^{-1}$. □

Remark 5.2.9. Let $\alpha = \sqrt{q} + t$, where $q \in \mathbb{Q}^+$, $t \in \mathbb{Q}$ and $\sqrt{q} \notin \mathbb{Q}$. Using the isomorphism $x \mapsto x^*$ (see 5.2.5(ii)) of $\mathbb{Q}[\alpha]$ and 5.2.8 we can state an analogical classification for the associated root $\alpha^* = -\sqrt{q} + t$ and $B = \mathbb{Q}^+[\alpha^*]$.

Corollary 5.2.10. *Let $\alpha \in \mathbb{C}$ be algebraic of degree 2. Then $\mathbb{Q}^+[\alpha]$ is a parasemifield if and only if there exist $q \in \mathbb{Q}^+$ and $t \in \mathbb{Q}^-$ such that $\sqrt{q} \notin \mathbb{Q}$, $\sqrt{q} > -t$ and either $\alpha = \sqrt{q} + t$ or $\alpha = -\sqrt{q} + t$.*

Moreover, if $\alpha = \sqrt{q} + t$, then $\mathbb{Q}^+[\alpha] = \mathbb{Q}[\sqrt{q}]^+$ and, if $\alpha = -\sqrt{q} + t$, then $\mathbb{Q}^+[\alpha] = \{a - b\sqrt{q} | a, b \in \mathbb{Q}, a > -b\sqrt{q}\}$.

Proof. Combine 5.2.4, 5.2.5(i), 5.2.8 and 5.2.9. □

Bibliography

[1] V. A. Andrunakievitch, *Semiradical rings*, Izvestia Akademii Nauk SSSR - Ser. Mat. **12** (1948), 129-178.

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

[3] S. Bulman-Fleming, E. Hotzel, J. Wang, *Semigroups that are factors of subdirectly irreducible semigroups by their monolith*, Algebra Universalis **51** (2004), 1-7.

[4] N. Divinsky, *Commutative subdirectly irreducible rings*, Proc. Amer. Math. Soc. **8** (1957), 642-648.

[5] N. Divinsky, *Pseudo-regularity*, Can. Jour. Math. **7** (1955), 401-410.

[6] K. Głazek, *A Guide to the Literature on Semirings and their Applications in Mathematics and Information Sciences*, Kluwer Academic Publishers, Dordrecht (2002).

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

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

[9] U. Hebisch, H. J. Weinert, *Semirings and semifields*, Handbook of Algebra Vol. **1**, Elsevier, Amsterdam (1996), 425-462.

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

[11] J. Ježek, T. Kepka, *The factor of a subdirectly irreducible algebra through its monolith*, Algebra Universalis **47** (2002), 319-327.

[12] J. Ježek, P. Marković, D. Stanovský, *Homomorphic images of finite subdirectly irreducible unary algebras*, Czech.Math.J. **57** (2007), 671-677.

[13] V. Kala, *Simple semirings*, bachelor thesis (2007).

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

[15] V. Kala, T. Kepka, M. Korbelář, *Notes on commutative parasemifields*, to appear in Comment. Math. Univ. Carolinae.

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

[17] T. Kepka, *A note on subdirectly irreducible grupoids*, Acta Univ. Carolinae - Math. and Phys. **22(1)** (1981), 25-28.

[18] T. Kepka, M. Korbelář, *Various examples of parasemifields*, to appear in Acta Univ. Carolinae - Math. and Phys.

[19] T. Kepka, P. Němec, *Commutative radical rings I*, Acta Univ. Carolinae - Math. and Phys. **48(1)** (2007), 11-41.

[20] Neal H. McCoy, *Subdirectly irreducible commutative rings*, Duke Math. J. **12(2)** (1945), 381-387.

[21] R. McKenzie, D. Stanovský, *Every quasigroup is isomorphic to a subdirectly irreducible quasigroup modulo its monolith*, Acta Sci. Math. (Szeged) **72** (2006), 59-64.

[22] D. Stanovský, *Homomorphic images of subdirectly irreducible grupoids*, Comment. Math. Univ. Carolinae **42(3)** (2001), 443-450.

[23] H. S. Vandiver, *Note on a simple type of algebra in which the cancellation law of addition does not hold*, Bull. Amer. Math. Soc. **40** (1934), 916-920.