SEMIRING CONGRUENCES AND TROPICAL GEOMETRY

by

Kalina Mincheva

A dissertation submitted to Johns Hopkins University in conformity with the requirements for the degree of Doctor of Philosophy

Baltimore, Maryland

20 March 2016

©Kalina Mincheva
All Rights Reserved

Abstract

One of the main motivations and inspirations for this thesis is the still open question of the definition of geometry in characteristic one. This is geometry over a structure, called an idempotent semiring, in which $1 + 1 = 1$. While mathematicians have studied semirings for many years, these structures have only recently ignited interest in algebraic geometry, more precisely tropical geometry. This is geometry over a particular idempotent semiring - the tropical semifield. Furthermore, semirings have important number theoretic applications which appear in the work of A. Connes and C. Consani which is focused on finding a new approach to the Riemann hypothesis.

We define the prime spectrum of a commutative semiring. Since ideals do not retain their distinguished role in the theory of semirings, the points of this spectrum correspond to certain congruence relations, which we call prime congruences. Motivated by tropical geometry, the key theme of our work is to study the prime spectrum of tropical polynomial semirings, but many of the results presented here apply to any additively idempotent semiring as well.

The class of prime congruences which we introduce turns out to exhibit some analogous properties to the prime ideals of commutative rings. In order to establish a good notion of radical congruences, we show that the intersection of all primes of a semiring can be characterized by certain twisted power formulas. We give a complete description of prime congruences in the polynomial and Laurent polynomial semirings over the tropical semifield $\mathbb{R}_{max}$, the semifield $\mathbb{Z}_{max}$ and the Boolean semifield $\mathbb{B}$. The minimal primes of these semirings correspond to monomial orderings, and their intersection is the congruence that identifies polynomials that have the same Newton polytope. We show that the radical of every finitely generated congruence in each of these cases is an intersection of prime congruences with quotients of Krull dimension 1. Using this setup we prove one of the main results of this thesis - we improve on a result of A. Bertram and R. Easton which can be regarded as a Nullstellensatz for tropical polynomials.

The remaining results are centered about the concept of Krull dimension. We prove that for any idempotent semiring A we have that $\dim A[x] = \dim A + 1$. In the case when we work over the tropical semifield, we relate the dimension of a tropical variety (which is just a polyhedral complex) to our Krull dimension. This shows the relevance of our notion in the context of the standard framework of tropical geometry.

Readers: Professor Dr. Caterina Consani (advisor), Dr. Jack Morava

Acknowledgments

I would would like to thank first and foremost my advisors Caterina Consani and Jack Morava for providing kind guidance and motivation throughout the development of this thesis. I would like to express my special thanks to my collaborator and best friend Daniel Joó for the countless long conversations about this project. Without his support, insight, kindness and patience this thesis would not have been possible.

I am very grateful to Jefferey Giansiracusa for the many conversations which inspired the last part of the chapter 7 of this thesis. I also want to thank my two academic brothers - Jaiung Jun and Jeffrey Tolliver, for the inspiring discussions and for pointing my attention to many useful papers.

I am grateful to Sam Payne for allowing me to be part of the conference on topical geometry at Yale in 2014 which was very inspirational and instrumental part for the development of this thesis.

I would like to thank my friends Jon Beardsley, Vitaly Lorman, Sven Cattell, Apurva Nakade, Sarah Inwood, Richard Brown and Jesus Martinez-Garcia. Their moral support, friendship and understanding have been very important throughout my graduate school studies.

Finally, I would like to express my deepest gratitude to my parents for their love and support every step of the way.

Contents

1

Introduction

1.1 History and Motivation

In this thesis we investigate the geometry over idempotent semirings from a new perspective. A semiring satisfies the same axioms that a ring does except invertibility of addition. A semifield is a semiring in which all nonzero elements have multiplicative inverse. One of the motivations for this study was understanding the geometry in characteristic one which is still an open question and has important arithmetic implications. Geometry over semirings is also interesting from the point of view of tropical geometry, which is geometry over the tropical semiring usually denoted by $\mathbb{T}$ or $\mathbb{R}_{max}$. As a set this semifield is $\mathbb{R} \cup \{-\infty\}$ with two operations maximum, playing the role of addition and usual addition playing the role of multiplication.

Tropical geometry is an area that recently has received a lot of interest and attention and has applications not just to algebraic geometry, but also to moduli spaces and compactifications ([Tev07], [RSS13]), mirror symmetry ([Gro10],[Gro11]) and mathematical biology ([PS04], [Man11]). Tropical methods are often used to approach hard classical algebraic geometry problems (cf. [Mik05], [JP15], [CDPR12]) but the tropical varieties are interesting on their own.

Classically ([MS], [Mik06]) a tropical variety is the tropicalization of a subvariety X of the n-dimensional torus over a field endowed with a non-Archimedean valuation. It is a degeneration of the original variety and can be thought of as its "combinatorial shadow". There are different ways to obtain the tropicalization of a variety. One approach is to apply the field valuation to each point of the original variety. Alternatively, one can obtain the tropicalization by considering coefficient-wise valuations of the defining polynomials of the original variety. Tropical varieties can also be understood through the theory of Berkovich spaces.

A priori a tropical variety is a balanced, wighted polyhedral complex and has no scheme structure. Recently there has been a lot of work aiming at finding the appropriate definition of a tropical scheme. The authors in [GG13] and [MR14] endow varieties defined over an idempotent semiring with a tropical scheme structure given by a particular congruence. The $\mathbb{T}$-points of these semiring schemes correspond to set-theoretic tropical varieties.

These results suggest why we should study congruences to understand the geometry over semifields. Furthermore, we explore the link to both tropical varieties and tropical schemes (as an example of semiring schemes) and develop the semiring algebra tools necessary to work with these objects.

The use of congruences in the study of tropical and semiring geometry has been taken up previously in the literature cf. [BE13], [Lor12]. The congruence approach was even proposed by Berkovich in [Ber11] in view of exploration of $\mathbb{F}_1$-geometry. While this is a more degenerate setting, for one considers multiplicative monoids instead of semirings, the geometry over the field of one element is historically an important step in the development of characteristic one geometry. In particular, the $\mathbb{F}_1$-theory developed by A. Deitmar in [Dei05] and [Dei08] provides a convenient language for working with monoids and semirings at the same time since there exists a base change functor from this $\mathbb{F}_1$-theory to every (semi)ring.

Apart from the tropical semifield, two other idempotent semifields are central to this thesis. The first one is denoted by $\mathbb{B}$ and is the smallest additively idempotent semifield. Its underlying set is $\{1, 0\}$, where 1 is the multiplicative identity, 0 is the additive identity and $1 + 1 = 1$. The second semifield denoted by $\mathbb{Z}_{max}$ is the subsemifield of integers of the tropical semifield. These two semifields are key to the semiring approach to characteristic one geometry. More precisely, $\mathbb{Z}_{max}$ is central to the work of A. Connes and C. Consani in [CC13] aiming at developing a correct framework for characteristic one geometry that is in congruence with the original idea of J. Tits [Tit56]. Their theory is furthermore used in the construction of the arithmetic site [CC14] and the scaling site [CC15]. In analogy with Weil's proof of the Riemann hypothesis for function fields the authors relate the Riemann zeta function to the problem of counting fixed points of a Frobenius action on the arithmetic site and show a Frobenius correspondences on the square of the arithmetic site.

1.2 Results

The objective of this thesis is to study the geometry over additively idempotent semirings and more precisely to understand sets defined by polynomial equations over these semirings. To accomplish this goal we study prime congruences in this setting. In the case of semirings congruences are a more natural object to consider than ideals. Unlike classical algebraic geometry ideals of semirings are no longer in bijection with the congruences of the base structure and do not play the same role as ideals in ring theory do.

The approach to understand geometry in the semiring setting using congruences has been previously considered by [BE13], [Les12] and [Lor12]. However, the structures that the authors obtain do not exhibit nice properties or do not capture a lot of geometric information. A possibility, which was investigated in [Les12], is to require that in the quotient by a prime congruence there are no zero divisors. The main drawback of this approach is that the prime property of a congruence solely depends on the equivalence class of the 0 element (i.e. the kernel of the congruence), which in general contains little information about the congruence itself. For example in a Laurent polynomial semiring over a semifield the kernel of every congruence is just $\{0\}$. A stricter way to define primes, as in [BE13] and [Lor12] is to require that their quotients are cancellative semirings, i.e. $ab = ac$ implies $a = 0$ or $b = c$. While this certainly is a narrower class, congruences with this property fail to be irreducible (under intersection) in general, making it difficult to treat them analogously to the primes of ring theory. Moreover most structures that are of interest to us will contain infinitely long chains of congruences with cancellative quotients, hence they do not provide a good notion of Krull dimension.

We propose a new definition of prime congruences. To develop the theory we use a product on elements of a congruence (ordered pairs), which is referred to as twisted product. The twisted product of two ordered pairs $\alpha = (a_1, a_2)$ and $\beta = (b_1, b_2)$ is the ordered pair $(a_1b_1+a_2b_2, a_1b_2+a_2b_1)$. Now we define a congruence P to be prime if it has the property that the twisted product of two ordered pairs lies in P if and only if one of them lies in P.

Using this definition we prove that our primes exhibit properties analogous to the primes in ring theory.

Theorem A. *For an additively idempotent semiring A a congruence $P \subset A \times A$ is prime if and only if it is irreducible (it can not be obtained as the intersection of two strictly larger congruences) and the quotient A/P is a cancellative semiring.*

We provide a complete description of prime congruences over the polynomial semirings with coefficients in one of the three semifields that are fundamental for the development of the theory of geometry over characteristic 1. These are the Boolean semifield $\mathbb{B}$, the semifield of tropical numbers $\mathbb{T}$ and its sub-semifield of integers $\mathbb{Z}_{max}$. It is easy to see that the quotient by a prime congruence is an ordered semifield. In the case of polynomial semirings with coefficients in $\mathbb{B}$ we can apply a result of Robbiano [Rob85] that a monomial ordering can be described by a matrix to obtain the following result.

Theorem B. *All prime congruences of the polynomial and Laurent polynomial semirings with coefficients in $\mathbb{B}$ are fully determined by a defining matrix, which is an admissible matrix with columns equal to the number of variables.*

We provide an analogous description of the prime congruences of the polynomial and Laurent polynomial semirings with coefficients in $\mathbb{Z}_{max}$ and $\mathbb{T}$. Furthermore, we also describe the minimal prime congruences in these cases in therms of their defining matrices.

The definition for prime congruences proposed in this thesis can be used to define Krull dimension for semirings. Just like in commutative algebra one can use the notion of prime ideals to compute Krull dimension, however it has been shown in a paper by [AA94] that even in the simplest case of a one variable polynomial semiring over the Boolean semifield the so defined Krull dimension is infinite. If instead one uses the existing notions in the literature of a prime congruence, that is a congruence whose quotient is a cancellative semifield, then one again obtains infinitely long chains of prime congruences.

The main result of this investigation is the following theorem, which concerns the polynomial semiring $A[x]$ and the Laurent polynomial semiring $A(x)$ over an arbitrary additively idempotent commutative semiring A (that is a $\mathbb{B}$-algebra).

Theorem C. *Let A be a $\mathbb{B}$-algebra with* $\dim A < \infty$. *Then we have that* $\dim A[x^{\pm 1}] = \dim A[x] = \dim A + 1$.

This result meets our intuitive expectations, since the semifield $\mathbb{B}$ is of dimension 0 and the semifields $\mathbb{Z}_{max}$ and $\mathbb{T}$ are of dimension 1. In the case when A is $\mathbb{B}$, $\mathbb{Z}_{max}$ and $\mathbb{T}$ this statement is shown directly in this thesis by investigating the chains of prime congruences.

One should note that an analogous result holds in classical ring theory - for any Noetherian ring R $\dim R[x] = \dim R + 1$. When the Noetherian condition is dropped then $\dim R[x]$ can be any integer between $\dim R + 1$ and $2 \dim R + 1$. Note that here the only condition on the semiring A is that it is additively idempotent.

The next natural step in understanding of the geometry over idempotent semirings is studying their radical congruences. We first provide a suitable notion of radical which is defined as the intersection of all prime congruences of a semiring. Similarly to commutative ring theory, the radical can be expressed using certain power formulas. However, in the semiring setting the twisted powers of pairs are not the correct equivalent to powers of elements in a ring. To alleviate the problem we define the set generalized powers $GP(\alpha)$ of an element of a congruence $\alpha = (\alpha_1, \alpha_2) \in A \times A$ to be the set of pairs $((\alpha_1 + \alpha_2)^i + h, 0)\alpha^j$, for any $h \in A$ and i, j positive integers.

Theorem D. *For any congruence I of a $\mathbb{B}$-algebra A, we have that*

$$Rad(I) = \{\alpha \in A \times A \mid GP(\alpha) \cap I \neq \emptyset\},$$

In particular, the intersection of all prime congruences of A is precisely the set of nilpotent pairs, that is the set of elements which have a twisted power in the diagonal.

The next part of this thesis provides an answer to a question raised in a paper by A. Bertram and R. Easton from 2013 about finding an analogue of Hilbert's Nullstellensatz for tropical polynomials.

Given a congruence C of the n-variable polynomial semiring $\mathbb{T}[\boldsymbol{x}]$ we consider the following set

$$\mathbb{V}(C) = \{v \in \mathbb{T}^k \mid f(v) = g(v), \, \forall (f, g) \in C\}.$$

Note that in classical algebraic geometry the set $\mathbb{V}(C)$ is just the vanishing locus of the ideal generated by $\langle f - g \rangle$, but for the lack of subtraction in a semifield we have to work with the original locus, namely the pairs (f, g). For a subset $H \subseteq \mathbb{T}^k$ we define the congruence

$$\mathbb{E}(H) = \{(f, g) \in \mathbb{T}[\boldsymbol{x}] \times \mathbb{T}[\boldsymbol{x}] \mid f(v) = g(v), \forall v \in H\}.$$

The aim of a "Tropical Nullstellensatz" is to describe the set $\mathbb{E}(\mathbb{V}(C))$ by implementing some suitable power formulas, when C is finitely generated. Recall that the classical Nullstellensatz states that $\boldsymbol{I}(V(J)) = \sqrt{J}$, where J is an ideal of a polynomial ring over an algebraically closed field and $\sqrt{J}$ is the radical of J, which is the intersection of all prime ideals lying above J.

A key component of the classical Nullstellensatz is that in a polynomial ring over a field every radical ideal is the intersection of maximal ideals. This statement does not hold for congruences of polynomial semirings, since there are very few maximal congruences. However, we obtained an analogous result if the maximal congruences are replaced with prime congruences with at most

1-dimensional quotient. A subset of these congruences, which have quotient $\mathbb{T}$ we call geometric congruences. The statement of the "tropical Nullstellensatz" can be summarized as the following theorem.

Theorem E. *For a finitely generated congruence C of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ or $\mathbb{T}[\boldsymbol{x}]$ we have that $\mathbb{E}(\mathbb{V}(C))$ is equal to the intersection of all geometric congruences containing C. Equivalently, $\mathbb{E}(\mathbb{V}(C))$ consists of all pairs of polynomials (f, g) for which one can find an $\epsilon \in \mathbb{T} \setminus \{1\}$, a non-negative integer i and a polynomial h such that $(1, \epsilon)((f + g, 0)^i + h)(f, g) \in C$.*

The weak tropical Nullstellensatz was proven in Theorem 2 of [BE13]. However, the statement easily follows from our theory. The tropical weak Nullstellensatz states that for a finitely generated congruence C of $\mathbb{T}[\boldsymbol{x}]$, the set $\mathbb{E}(\mathbb{V}(C))$ is empty if and only if there exists a polynomial $h \in \mathbb{T}[\boldsymbol{x}]$ with nonzero constant term such that $(h, \epsilon h) \in C$ for some $\epsilon \in \mathbb{T}$.

A different approach to the Nullstellensatz problem was taken in [IR14], where so-called supertropical structures were studied in order to establish the Zariski correspondence between congruences of tropical polynomials and algebraic sets.

The last part of this thesis explores the link between the sets $\mathbb{V}(C)$ and the tropical varieties defined in [MS] and the tropical schemes as defined if [GG13]. We apply the theory developed in the current work to tropical varieties regarding them as $\mathbb{V}(C)$, where C is the defining congruence of a the tropical scheme. For a classical affine variety X over a valued field defined by an ideal I, we have that

$$trop(X) = trop(V(I)) = Hom(\mathbb{T}[\boldsymbol{x}^{\pm 1}]/Bend(I), \mathbb{T}) = \mathbb{V}(Bend(I)),$$

where $Bend(I)$ a congruence on the $\mathbb{T}$-linear span of coefficient-wise valuations of elements of I, called the bend congruence. Moreover, we prove a connection between the dimension of the original variety and the Krull dimension of the congruence $Bend(I)$:

$$\dim X = \dim \mathbb{T}[\boldsymbol{x}]/Bend(I) - 1.$$

In the last part of the thesis we investigate the group $Hom(\mathbb{T}[\boldsymbol{x}^{\pm 1}]/Bend(I), \mathbb{T}_n)$, for all n, where $\mathbb{T}_n$ as a set is $\mathbb{R}^n_{lex} \cup \{-\infty\}$ with operations lexicographical order and vector addition.

2

Preliminaries

In this section we provide some background on tropical geometry and characteristic one geometry and give context for the subsequent results. We first introduce set theoretic tropicalization and then we discuss the construction of tropical schemes.

2.1 Tropical Geometry and Set Theoretic Tropicalization

We begin by introducing the tropical semifield which we will denote by $\mathbb{T}$. There are two ways to define $\mathbb{T}$. For this thesis the underlying set of $\mathbb{T}$ is $\mathbb{R} \cup \{-\infty\}$ and it has two binary operations - tropical sum being the maximum of two real numbers and tropical product being usual addition. This object is also denoted by $\mathbb{R}_{max}$ in the literature. Note that $\mathbb{T}$ satisfies all axioms for a field except invertibility of addition. Alternatively one can define the tropical semifield to be $\mathbb{R} \cup \{\infty\}$ with operations minimum and addition, we denote this object by $\mathbb{R}_{min}$. This semiring is additively idempotent, that is $a + a = a, \ \forall a \in \mathbb{T}$.

Let K be a field with a non-Archimedean valuation ν, that is a map $\nu : K \to \mathbb{R} \cup \{-\infty\} = \mathbb{T}$ which satisfies the following conditions:

- $\nu(a) = -\infty \iff a = 0$
- $\nu(ab) = \nu(a) + \nu(b)$
- $\nu(a + b) \leq max\{\nu(a), \nu(b)\}$ for all $a, b \in K^*$.

We will denote by R_K the set of all field elements with non-negative valuation $R_K = \{a \in K : \nu(a) \geq 0\}$. The set R_K is a local ring with maximal ideal $m_K = \{a \in K : \nu(a) > 0\}$. The residue field we denote by $\daleth = R_K/m_K$.

We denote by Γ_ν the image of the valuation map. The field K is not required to be algebraically closed, but we will assume that the valuation ν is nontrivial and that the value group Γ_ν is dense in $\mathbb{R}$. Furthermore, we would assume that there is a splitting $\phi : \Gamma_\nu \to K^*$, $\omega \mapsto t^\omega$. If $\nu(a) \geq 0$, we denote by $\overline{a}$ the image of a in the residue field $\daleth$. For a polynomial f with coefficients in R, $\overline{f}$ denotes the polynomial obtained by replacing every coefficient a by $\overline{a}$.

Let $K[\boldsymbol{x}^{\pm 1}]$ denote the ring of Laurent polynomials over K and let $f = \sum_{u \in \mathbb{Z}^n} c_{\boldsymbol{u}} x^{\boldsymbol{u}}$ be a Laurent polynomial. The tropicalization of f denoted by $trop(f)$ is a piecewise linear function defined by

$$trop(f)(\boldsymbol{w}) = max\{\nu(c_{\boldsymbol{u}}) + \sum_{i=1}^{n} u_i w_i\} = max\{\nu(c_{\boldsymbol{u}}) + \boldsymbol{u} \cdot \boldsymbol{w} \ : c_{\boldsymbol{u}} \neq 0\}.$$

Now we are ready to define tropical hyper surface. Recall that if $f \in K[x_1^{\pm 1}, \dots x_n^{\pm 1}]$, where K is algebraically closed, then the zero locus of f is a hypersurface in the n-dimensional algebraic torus.

Definition 2.1.1 ([MS] Definition 3.1.1)**.** *The tropical hypersurface $trop(V(f))$ is the set of all $\boldsymbol{w} \in \mathbb{R}^n$ for which the maximum in $trop(f)$ is achieved at least twice.*

Example 2.1.2. Let K be a field with trivial valuation and $f = x + y + 1 \in K[x, y]$, and $X := V(f)$. We have that $trop(f) = max\{x, y, 0\}$. The tropical hypersurface in this case is:

$$trop(V(f)) = \{(a, b) \in \mathbb{R}^2 |\ a = b \geq 0\} \cup \{(a, b) \in \mathbb{R}^2 |\ a = 0 \geq b\} \cup \{(a, b) \in \mathbb{R}^2 |\ b = 0 \geq a\}.$$

The set of points of the tropical line is the union of the three colored half lines below.

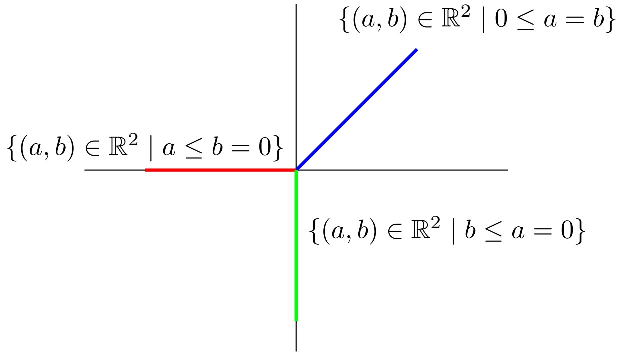
$\{(a,b) \in \mathbb{R}^2 \mid 0 \leq a = b\}$
$\{(a,b) \in \mathbb{R}^2 \mid a \leq b = 0\}$
$\{(a,b) \in \mathbb{R}^2 \mid b \leq a = 0\}$

Figure 1. Tropical Line in $\mathbb{R}^2$

When F is a tropical polynomial we write $V(F)$ for the set of points $w \in \mathbb{R}^n$ where the minimum in F is achieved at least twice. Thus we have $trop(V(f)) = V(trop(f))$.

We can also define tropical hypersurfaces in terms of initial forms.

The initial form for f is

$$in_{\boldsymbol{w}}(f) = \sum_{\substack{u:\nu(c_{\boldsymbol{u}})+\boldsymbol{u}\cdot\boldsymbol{w} \\ =trop(f)(\boldsymbol{w})}} \overline{t^{-\nu(c_u)}c_{\boldsymbol{u}}} x^{\boldsymbol{u}}.$$

Now we can introduce the following theorem.

Theorem 2.1.3 ([MS] Theorem 3.1.3 (Kapranov's theorem))**.** *Let $f = \sum_{u\in\mathbb{Z}^n} c_{\boldsymbol{u}}x^{\boldsymbol{u}}$ be a Laurent polynomial in $K[x_1^{\pm 1}, \ldots x_n^{\pm 1}]$. Then the following sets coincide:*

a) the tropical hypersurface $trop(V(f)) \in \mathbb{R}^n$

b) the closure in $\mathbb{R}^n$ of the set of $\boldsymbol{w} \in \Gamma_\nu^n$ for which $in_{\boldsymbol{w}}(f)$ is not a monomial.

c) the closure in $\mathbb{R}^n$ of $\{(\nu(y_1), \ldots, \nu(y_n)) : (y_1, \ldots, y_n) \in V(f)\}$.

Now we are ready to move from tropical hypersurfaces to tropical varieties.

Definition 2.1.4 ([MS] Definition 3.2.1)**.** *Let I be an ideal in the Laurent polynomial ring and $K[x_1^{\pm 1}, \ldots x_n^{\pm 1}]$ let $X = V(I)$ be the variety defined by this ideal in the algebraic n-torus. The tropicalization $trop(X)$ of the variety X is the intersection of all tropical hypersurfaces defined by Laurent polynomials in the ideal I. That is,*

$$trop(X) = \bigcap_{f\in I} trop(V(f)) \subseteq \mathbb{R}^n.$$

In fact, it is enough if we take the intersection of a finite number of hypersurfaces. For this we need to define tropical basis. The tropical basis is an analogue to universal Gröbner basis for $K[x_1^{\pm 1}, \ldots x_n^{\pm 1}]$.

Definition 2.1.5 ([MS] Definition 2.6.4)**.** *Let I be an ideal in the Laurent polynomial ring $K[x_1^{\pm 1}, \ldots x_n^{\pm 1}]$ over a valued field K. A finite generating set $\mathcal{T}$ of I is said to be a tropical basis for I if for all weight vectors $\boldsymbol{w} \in \Gamma_{val}^n$, the initial ideal $in_{\boldsymbol{w}}(I)$ contains a unit if and only if $in_{\boldsymbol{w}}(\mathcal{T}) = \{in_{\boldsymbol{w}}(f) : f \in \mathcal{T}\}$ contains a unit.*

Example 2.1.6. Consider the ideal $I = \langle x+y+1, x+2y\rangle$ in $K[x^{\pm 1}, y^{\pm 1}]$, where $K = \mathbb{C}\{\{t\}\}$ - the field of Puiseux series with the usual valuation on it. Then the following set is a tropical basis for I:

$$\mathcal{T} = \{x+y+1, x+2y, y-1\}.$$

Theorem 2.1.7 ([MS] Theorem 2.6.5)**.** *Every ideal I in the Laurent polynomial ring $K[x_1^{\pm 1}, \ldots x_n^{\pm 1}]$ has a finite tropical basis $\mathcal{T}$.*

Corollary 2.1.8 ([MS]Corollary 3.2.3)**.** *Let $\mathcal{T}$ be a tropical basis of the ideal I then*

$$trop(X) = \bigcap_{f \in \mathcal{T}} trop(V(f)).$$

Now we can introduce a generalization of Kapranov's theorem to arbitrary tropical varieties.

Theorem 2.1.9 ([MS] Theorem 3.2.5 (Fundamental Theorem of Tropical Algebraic Geometry))**.** *Let I is an ideal in the Laurent polynomial ring $K[x_1^{\pm 1}, \dots x_n^{\pm 1}]$ and $X = V(I)$ is a subvariety of the algebraic n-torus $(K^*)^n$. Then the following sets coincide:*

a) the tropical variety $trop(X)) \in \mathbb{R}^n$

b) the closure in $\mathbb{R}^n$ of the set of $\boldsymbol{w} \in \Gamma_\nu^n$ for which $1 \notin in_{\boldsymbol{w}}(I)$

c) the closure in $\mathbb{R}^n$ of $\{(\nu(y_1), \dots, \nu(y_n)) : (y_1, \dots, y_n) \in X\}$.

Next we introduce the Structure Theorem for tropical varieties. We would first need to define the following two concepts. Let $\Sigma \in \mathbb{R}^n$ be a one-dimensional rational fan with s rays and $\boldsymbol{u}_i$ be the first lattice point on the i-th ray of Σ. Then we can assign a positive integer weight $m_i \in \mathbb{N}$ to the i-th ray of Σ, turning Σ into a weighted fan. We say that the fan Σ is balanced if $\sum m_i \boldsymbol{u}_i = 0$.

Theorem 2.1.10 ([MS] Theorem 3.3.6 (Structure Theorem for Tropical Varieties))**.** *Let X be an irreducible subvariety of the n-torus T^n of dimension d. Then $trop(X)$ is the support of a balanced weighted Γ_ν-rational polyhedral complex pure of dimension d. Moreover, that polyhedral complex is connected through codimension one.*

Thus every topical variety comes with a set of multiplicities. Note that if $f = x + y + 1$ and $g = x^3 + y^3 + 1$, then points of the tropicalizations of $V(f)$ and $V(g)$ are the same but these two tropical hypersurfaces have different multiplicities.

Definition 2.1.11 ([MS] Definition 3.4.3.)**.** *Let I be an ideal in $K[x_1^{\pm 1}, \dots x_n^{\pm 1}]$. Let Σ be a polyhedral complex with support $trop(V(I))$ such that $in_{\boldsymbol{w}}(I)$ is constant for $\boldsymbol{w} \in relint(\sigma)$ for all $\sigma \in \Sigma$. For a polyhedron $\sigma \in \Sigma$ maximal with respect to inclusion, the multiplicity $mult(\boldsymbol{w})$ is defined by*

$$mult(\sigma) = \sum_P mult(P, in_{\boldsymbol{w}}(I)),$$

where the sum runs over the minimal associate primes of $in_{\boldsymbol{w}}(I)$ and $mult(P, in_{\boldsymbol{w}}(I))$ is the multiplicity of the associated primary component.

Finally we recall a result about tropical hypersurfaces in the case when the valuation of the coefficients of the defining Laurent polynomial f are all 0.

Proposition 2.1.12 ([MS] Proposition 3.1.10)**.** *Let $f \in K[x_1^{\pm 1}, \dots x_n^{\pm 1}]$ be a Laurent polynomial whose coefficients all have valuation zero. Then the tropical hypersurface trop$(V(f))$ is the support of an $(n-1)$-dimensional polyhedral fan in $\mathbb{R}^n$. That fan is the $(n-1)$-skeleton of the normal fan to the Newton polytope of f.*

2.2 Scheme Theoretic Tropicalization

We proceed with the construction of semiring schemes and in particular tropical schemes, as introduced in [GG13]. We recall that a semiring is a set with two binary operations, which satisfy the ring axioms except invertibility of addition.

For a semiring A we can define the prime (ideal) spectrum of A in the usual way. Ideals and modules of semirings are defined analogously to those of rings. An ideal of A is prime if it is proper and if its complement is closed under multiplication. We can define localization by (the complement of) a prime ideal $\mathfrak{p}$, which is denoted as usual by $A_{\mathfrak{p}}$. The set of prime ideals $SpecA$ is equipped with the Zariski topology. Analogously to the classical situation, closed sets are the collections of primes containing a certain ideal. We have the usual base for the topology of affine open sets $D(f) = \{\mathfrak{p} |\ f \notin \mathfrak{p}\}$, for $\mathfrak{p} \in SpecA$. The structure sheaf $\mathcal{O}_{SpecA}$ is defined analogously to classical affine schemes.

An affine scheme over a semiring algebra Q is a pair $(X, \mathcal{O})$ where X is topological space and $\mathcal{O}$ is a sheaf of Q-algebras where the pair $(X, \mathcal{O})$ is isomorphic to a pair of the form $(SpecA, \mathcal{O}_{Spec(A)})$. A general Q-scheme is a pair that is locally affine. If Q is a ring, this definition gives back the usual definition for schemes.

Defining closed subschemes in the case of semiring schemes is different from the classical case. If R is a ring and the corresponding affine scheme $SpecR$, then $Spec(R/I)$ is a closed subscheme for some ideal $I \subset R$. However as previously noted, in the case when A is a semiring, there is no bijection between ideals and congruences. To obtain a semiring subscheme of $SpecA$ one needs to consider the quotient A/C, where C is a congruence on A.

A priori tropical varieties do not have scheme structure. A tropical schemes associated to a classical variety X is denoted by $\mathcal{T}rop(X)$.To talk about scheme theoretic tropicalization we need the following definition.

Definition 2.2.1 (adapted from [GG13] Definition 5.1.1)**.** *Let S be an idempotent semiring and $f \in S[\boldsymbol{x}]$. For a in the support of f denoted by $supp(f)$, we write $f_{\hat{a}}$ for the result of deleting the a term from f. Then the bend relations of f are*

$$\{f \sim f_{\hat{a}}\}_{a \in supp(f)}.$$

The S-module congruence on $S[\boldsymbol{x}]$ generated by the bend relations of f is denoted by $B(f)$ and the S-module congruence generated by the bend relations for every $f \in J$ for an ideal $J \in S[\boldsymbol{x}]$ is denoted by $B(J)$.

Let J be an ideal of $K[\boldsymbol{x}]$, where K is a valued field with valuation $\nu : K \to \mathbb{T}$. We will denote by $\nu(f)$ the coefficient-wise valuation of a polynomial f, making $\nu(f)$ a polynomial in $\mathbb{T}$. We would not denote it by $trop(f)$ to emphasize that we are interested in the resulting polynomial not the function.

Let I be an ideal of $K[x^{\pm 1}]$, where K a valued field with valuation $\nu : K \to \mathbb{T}$. We will denote by $Bend(I)$ the congruence generated by the bend relations of the coefficient-wise valuations of all elements of I, that is the congruence generated by bend relations of $\nu(f)$, for every $f \in I$. For $f \in K[x^{\pm 1}]$ we will denote by $Bend(f)$ the congruence generated by the bend relations of $\nu(f)$.

Remark 2.2.2. Let J be an ideal of $K[\boldsymbol{x}]$, where K is a valued field with valuation $\nu : K \to \mathbb{T}$. It is important to note that if J is generated by the finite set of polynomials $\{f_1, \ldots, f_n\}$ then the bend relations of $\nu(f_i), 1 \leq i \leq n$ do not generate $Bend(J)$ even in the case when J is a principal ideal. This is best illustrated by the following example.

Example 2.2.3 (adapted from [GG13] Example 8.1.1.)**.** Let $f = x^2 + xy + y^2 \in k[x, y]$, where k is a valued field with valuation $\nu : k \to \mathbb{T}$. Denote by J the ideal generated by f. The bend congruence $Bend(J)$ is strictly larger than the congruence generated by the bend relations of $\nu(f)$, namely $Bend(f)$, where $\nu(f)$ is the tropical polynomial $max\{\nu(c_{\boldsymbol{u}}) + \boldsymbol{u} \cdot \boldsymbol{x}\}$. The congruence $Bend(f)$ is generated by the degree 2 relations

$$x^2 + y^2 \sim x^2 + xy \sim xy + y^2.$$

The degree 3 part is generated by the bend relations of the polynomials $x^3 + x^2y + xy^2$ and $x^2y + xy^2 + y^3$. Any nontrivial degree 3 relation in $Bend(f)$. involves only polynomials with at least 2 terms. However, $(x - y)f \in J$ and $(x - y)f = x^3 - y^3$, and this gives the degree 3 monomial relation in $Bend(J)$, namely $x^3 \sim y^3$, which is clearly not in $Bend(f)$.

Now we are ready to define scheme-theoretic tropicalization and tropical schemes. Let X be a closed affine scheme defined by an ideal I over a valued field k and let $\nu : k \to \mathbb{T}$ be a non-Archimedean valuation. Then the scheme theoretic tropicalization of X is defined to be $\mathcal{T}rop(X) = Spec\, \mathbb{T}[\boldsymbol{x}]/Bend(I)$. This construction can be globalized. The tropicalization construction commutes with monomial localizations (cf. [GG13] Lemma 6.1.5.) and affine pieces can be patched together. Now, for a scheme X over a valued field k we have that $\mathcal{T}rop(X)(\mathbb{T}) = trop(X)$.

One can determine the multiplicities from the tropical scheme.

Theorem 2.2.4 ([MR14] (part of) Theorem 1.2)**.** *Let K be a valued field with a valuation $\nu : K \to \mathbb{T}$ and Y a subscheme of the n-torus $(K^*)^n$ defined by an ideal $I \subset K[x_1^{\pm 1}, \dots x_n^{\pm 1}]$, then any of the following sets determines the others:*

a) The congruence $Bend(I)$, generated by the bend relations of coefficient-wise valuations of all polynomials of I.

b) The ideal $trop(I) \subset \mathbb{T}[x_1^{\pm 1}, \dots x_n^{\pm 1}]$, where $trop(I) = \langle \nu(f) = max\{\nu(c_{\boldsymbol{u}}) + \boldsymbol{u} \cdot \boldsymbol{x}\} : \ f \in I \rangle$.

Roughly speaking, we can recover the multiplicities of the tropical variety from the tropical scheme because tropicalization commutes with initial forms. (cf. [MR14] Lemma 3.3, 3.4)

3

Congruences

In this chapter we discuss the main building blocks for our framework - congruences. In the case of idempotent semirings congruences are a more natural object to consider than ideals.

Thus it is only natural to seek a suitable notion of a prime congruence. To define primes we use a so called twisted product on pairs elements of a congruence. The twisted product of two ordered pairs (a, b) and (c, d) is the ordered pair $(ac + bd, ad + bc)$. Following this characterization we define primes to be the congruences that do not contain twisted product of pairs that lie outside the congruence. We prove that a congruence is prime if and only if it cannot be written as a finite intersection of primes that strictly contain it and the quotient by it is a cancellative semirings. Thus the prime congruences exhibit analogous properties as the prime ideals in ring theory and are the natural choice for defining Krull dimension which is discussed in detail in the next chapter.

In the second part of this chapter we study radical congruences as a natural component in understanding geometry over semifields. The set $Rad(I)$ is defined as the intersection of all primes that contain the congruence I. We introduce certain twisted power formulas called generalized powers for ordered pairs, and show in Theorem 3.2.10 that the elements of a pair are congruent in $Rad(I)$ precisely when some generalized power of that pair lies in I.

3.1 Prime congruences of semirings

In this paper by a *semiring* we mean a commutative semiring with multiplicative unit, that is a nonempty set R with two binary operations $(+, \cdot)$ satisfying:

(i) $(R, +)$ is a commutative monoid with identity element 0

(ii) $(R, \cdot)$ is a commutative monoid with identity element 1

(iii) For any $a, b, c \in R$: $a(b + c) = ab + ac$

(iv) $1 \neq 0$ and $a \cdot 0 = 0$ for all $a \in R$

A *semifield* is a semiring in which all nonzero elements have multiplicative inverse. We will denote by $\mathbb{B}$ the semifield with two elements $\{1, 0\}$, where 1 is the multiplicative identity, 0 is the additive identity and $1 + 1 = 1$. The *tropical semifield* $\mathbb{T}$ - sometimes also denoted by $\mathbb{R}_{max}$ - is defined on the set $\{-\infty\} \cup \mathbb{R}$, by setting the + operation to be the usual maximum and the $\cdot$ operation to be the usual addition, with $-\infty$ playing the role of the 0 element. In this paper we will use the exponential notation $t^c,\ c \in \mathbb{R}$ for the elements of $\mathbb{T}$, allowing us to write $1 = t^0$ for the multiplicative identity element and 0 for the additive identity element. The semifield $\mathbb{Z}_{max}$ is just the subsemifield of integers in $\mathbb{T}$.

A polynomial (resp. Laurent polynomial) ring with variables $\boldsymbol{x} = (x_1, \ldots, x_k)$ over a semifield F is the semiring, denoted by $F[\boldsymbol{x}]$ (resp. $F(\boldsymbol{x})$), whose elements are formal linear combinations of the monomials $\{x_1^{n_1} ... x_k^{n_k} \mid n_i \in \mathbb{N}\}$ (resp. $\{x_1^{n_1} ... x_k^{n_k} \mid n_i \in \mathbb{Z}\}$) with coefficients in F, with addition and multiplication being defined in the usual way. For an integer vector $\boldsymbol{n} = (n_1, \ldots, n_k)$ we will use the notation $\boldsymbol{x}^{\boldsymbol{n}} = x_1^{n_1} ... x_k^{n_k}$.

As usual, an *ideal* in the semiring R is just a subsemiring that is closed under multiplication by any element of R. Congruences of semirings are just operation preserving equivalence relations.

Definition 3.1.1. A *congruence* I of the semiring R is a subset of $R \times R$ satisfying

(C1) For $a \in R$, $(a, a) \in I$

(C2) $(a, b) \in I$ if and only if $(b, a) \in I$

(C3) If $(a, b) \in I$ and $(b, c) \in I$ then $(a, c) \in I$

(C4) If $(a, b) \in I$ and $(c, d) \in I$ then $(a + c, b + d) \in I$

(C5) If $(a, b) \in I$ and $(c, d) \in I$ then $(ac, bd) \in I$

The unique smallest congruence is the diagonal of $R \times R$ which is denoted by Δ, also called the *trivial congruence.* In commutative algebra it corresponds to the zero ideal. $R \times R$ itself is the *improper congruence* the rest of the congruences are called *proper.*

If I is an ideal and we denote by C_I the congruence generated by the pairs $(a, 0)$, for every $a \in I$. Quotients by congruences can be considered in the usual sense, the quotient semiring of R

by the congruence I is denoted by R/I. Recall that in commutative algebra for an ideal I then $R/I := R/C_I$.

The *kernel* of a congruence is just the equivalence class of the 0 element. For a congruence $C \subseteq R \times R$

$$Ker(C) = \{a \in R | (a, 0) \in C\}.$$

The kernel of a congruence is always an ideal, and when we say that the kernel of a congruence is generated by some elements, we will mean it is generated as an ideal by those elements. We will say that the kernel of a congruence is trivial if it equals $\{0\}$.

In an idempotent semiring we have

$$(a + b, 0) \in C \Rightarrow (a, 0) \in C.$$

So whenever $(a+b) \in Ker(C)$ we also have $a \in Ker(C)$ and $b \in Ker(C)$. Ideals with these property are called *saturated*. Note that every saturated ideal is the kernel of a congruence. In general the congruence C_I is bigger than the set $\{(a, 0), \forall a \in I\}$. The smallest saturated ideal I^s that contains I for which $C_I = C_{I^s} = \{(a, 0), \forall a \in I^s\}$ is the *saturated closure* of I. The following is an example of $I \subsetneq I^s$,

Example 3.1.2. Consider the ideal $I = \langle x + 1\rangle \in \mathbb{B}[x]$ is clearly a proper ideal, but C_I is improper and $I^s = \mathbb{B}[x]$.

In general $Ker(C)$ contains little information about the congruence C. Note that kernels do not determine the congruences, for instance non-trivial congruences can have $\{0\}$ as their kernel as in the following example.

Example 3.1.3. Let $R = \mathbb{T}[x, y]$ and $C = \langle (x, y)\rangle$. $Ker(C) = \{0\}$ but C is a non-trivial congruence and $\mathbb{T}[x, y]/C \cong \mathbb{T}[x]$.

Thus there is no bijection between ideals and congruences as in ring theory.

As usual, if $\varphi : R_1 \to R_2$ is a morphism of semirings, and I is a congruence of R_2, the preimage of I is the congruence $\varphi^{-1}(I) = \{(\alpha_1, \alpha_2) \in R_1 \times R_1 \mid (\varphi(a_1), \varphi(a_2)) \in I\}$. By the *kernel of a morphism* φ we mean the preimage of the trivial congruence $\varphi^{-1}(\Delta)$, it will be denoted by $Ker(\varphi)$. If R_1 is a subsemiring of R_2 then the restriction of a congruence I of R_2 to R_1 is $I|_{R_1} = I \cap R_1 \times R_1$.

By a $\mathbb{B}$-algebra we simply mean a commutative semiring with idempotent addition (that is $a + a = a, \forall a$). Throughout this section A denotes an arbitrary $\mathbb{B}$-algebra. Note that the idempotent addition defines an ordering via

$$a \geq b \iff a + b = b.$$

Elements of $A \times A$ are called *pairs*. We denote pairs by Greek letters, and denote the coordinates of the pair α by α_1, α_2. The *twisted product* of the pairs $\alpha = (\alpha_1, \alpha_2)$ and $\beta = (\beta_1, \beta_2)$ is

$$\alpha\beta = (\alpha_1\beta_1 + \alpha_2\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1).$$

Note that the twisted product is associative and the pairs form a monoid under under this operation, with the pair $(1, 0)$ being the identity element. For the rest of the paper in any formula containing pairs the product is always the twisted product, so the twisted product of α and β is simply denoted by $\alpha\beta$. Similarly α^n denotes the twisted n-th power of the pair α, and we use the convention $\alpha^0 = (1, 0)$. The product of two congruences I and J is defined as the congruence generated by the set $\{\alpha\beta \mid \alpha \in I \, \beta \in J\}$. For an element a and a pair α we define their product as $a(\alpha_1, \alpha_2) = (a\alpha_1, a\alpha_2)$ which is the same as the twisted product $(a, 0)\alpha$.

The following elementary properties of congruences play an important role,

Proposition 3.1.4. *Let I be a congruence of A,*

(i) For $\alpha \in I$ and an arbitrary pair β we have $\alpha\beta \in I$.

(ii) For any two congruences I and J we have $IJ \subseteq I \cap J$.

(iii) If $(a, b) \in I$ and $a \leq c \leq b$ then $(a, c) \in I$ and $(b, c) \in I$. In particular if $(a, 0) \in I$ then for every $a \geq c$ we have $(c, 0) \in I$.

Proof. (i) follows immediately from the definition of a congruence and (ii) follows from (i). For (iii) consider that in A/I we have that

$$a = b \Rightarrow c = a + c = b + c = b = a.$$

□

Proposition 3.1.4 has the following important consequence:

Proposition 3.1.5. *If F is an additively idempotent semifield then every proper congruence in the semiring of Laurent polynomials $F(x_1, \dots, x_n)$ has a trivial kernel.*

Proof. If $f \in F(x_1, \dots, x_n)$ is in the kernel of a proper congruence I then by (ii) of Proposition 3.1.4 we also have that every monomial that appears in f is in the kernel of I. On the other hand every monomial in a Laurent semiring over a semifield has multiplicative inverse. Hence if a monomial is in the kernel of a congruence I then so is the multiplicative identity of $F(x_1, \dots, x_n)$, which implies that I is improper. □

One can readily show that for usual commutative rings, an ideal is prime if and only if the corresponding congruence does not contain twisted products of pairs lying outside. In particular, if P is an ideal of a commutative ring and C_P is the congruence with kernel P, then P is prime if and only if whenever $\alpha\beta \in C_P$ either $\alpha \in C_P$ or $\beta \in C_P$. This can be verified by checking that

$$\alpha\beta \in C_P \Leftrightarrow ((\alpha_1 - \alpha_2)(\beta_1 - \beta_2), 0) \in C_P \Leftrightarrow (\alpha_1 - \alpha_2)(\beta_1 - \beta_2) \in P.$$

This observation motivates the following definition.

Definition 3.1.6. We call a congruence P of a $\mathbb{B}$-algebra A prime if it is proper and for every $\alpha, \beta \in A \times A$ such that $\alpha\beta \in P$ either $\alpha \in P$ or $\beta \in P$. We call a $\mathbb{B}$-algebra a domain if its trivial congruence is prime.

We define dimension similarly to the Krull-dimension in ring theory:

Definition 3.1.7. By *dimension* of a $\mathbb{B}$-algebra A we will mean the length of the longest chain of prime congruences in $A \times A$ (where by length we mean the number of strict inclusions). The dimension of A will be denoted by $\dim(A)$.

Remark 3.1.8. For the above definition to make sense one needs to verify that every $\mathbb{B}$-algebra A has at least one prime congruence. Indeed it is a known fact that $\mathbb{B}$ is the only simple $\mathbb{B}$-algebra (i.e. the only proper congruence is the trivial one). Hence by the usual Zorn's lemma argument we see that every $\mathbb{B}$-algebra has a proper congruence with quotient $\mathbb{B}$, and it follows from the definition that such a congruence is prime.

For the sake of completeness we provide a short proof of the above fact:

Proposition 3.1.9. *The only simple* $\mathbb{B}$*-algebra is* $\mathbb{B}$.

Proof. First assume that A is a $\mathbb{B}$-algebra without zero-divisors. Then the map $\varphi : A \to \mathbb{B}$ defined as $\varphi(x) = 1$ for $x \neq 0$ and $\varphi(0) = 0$ is a homomorphism of $\mathbb{B}$-algebras. Hence $Ker(\varphi)$ is a proper congruence of A, which can only be trivial when $A \simeq \mathbb{B}$. Now assume that there are - not necessarily distinct - non-zero elements $x, y \in A$ such that $xy = 0$. Let I be the congruence generated by the pair $(x, 0)$. It follows from Lemma 3.2.8 that $(\alpha_1, \alpha_2) \in I$ if and only if there is an $r \in A$, such that $\alpha_1 + rx = \alpha_2 + rx$. Now we claim that $(1, 0) \notin I$. Indeed otherwise there would be an $r \in A$ such that $1 + rx = rx$ and multiplying both sides by y we would get $y = 0$, a contradiction. Hence I is a non-trivial proper congruence of A. □

The above Proposition can be reformulated in the following way.

Proposition 3.1.10. *(i) Every $\mathbb{B}$-algebra maps surjectively onto $\mathbb{B}$.*

(ii) The only $\mathbb{B}$-algebra that is a domain and has dimension 0 is $\mathbb{B}$.

A congruence is called *irreducible* if it can not be obtained as the intersection of two strictly larger congruences.

Proposition 3.1.11. *If a congruence is prime then it is irreducible.*

Proof. Indeed if P is the intersection of the strictly larger congruences I and J, then take $\alpha \in I \setminus P$ and $\beta \in J \setminus P$. Now by part (i) of Proposition 3.1.4 we have that $\alpha\beta \in I \cap J = P$ so P can not be prime. □

A $\mathbb{B}$-algebra A is called *cancellative* if whenever $ab = ac$ for some $a, b, c \in A$ then either $a = 0$ or $b = c$. The *annihilator* of a pair α is defined as $Ann_A(\alpha) = \{\beta \in A \times A \mid \alpha\beta \in \Delta\}$. $Ann_A(\alpha)$ satisfies the axioms (C1)-(C2) and (C4)-(C5) of a congruence but in general it is not transitive, consider the following example:

Example 3.1.12. Let A be the algebra $\mathbb{B}[x, y]/\langle (y, y^2) \rangle$. Then it is easy to check that $(y, x + 1), (y, 1) \in Ann_A((x, x + y))$ but $(1, x + 1) \notin Ann_A((x, x + y))$.

The annihilator of an element $a \in A$ is defined as the annihilator of the pair $(a, 0)$ and is also denoted by $Ann_A(a)$. It is easy to verify the following properties:

Proposition 3.1.13. *(i) For any $a \in A$, $Ann_A(a) = \{\beta \in A \times A \mid a\beta_1 = a\beta_2\}$, moreover $Ann_A(a)$ is a congruence.*

(ii) A is cancellative if and only if for every element $a \neq 0$ we have $Ann_A(a) = \Delta$, and a domain if and only if for every pair $\alpha \notin \Delta$ we have $Ann_A(\alpha) = \Delta$.

(iii) For a congruence I the quotient A/I is cancellative if and only if for every element a and pair α such that $(a, 0)\alpha \in I$ either $(a, 0) \in I$ or $\alpha \in I$.

(iv) If P is a prime congruence, then A/P is cancellative.

(v) If P is a prime congruence of A_1, $\varphi : A_2 \to A_1$ is a morphism of $\mathbb{B}$-algebras and A_3 is a subalgebra of A_1, then $\varphi^{-1}(P)$ and $P|_{A_3}$ are prime congruences.

We will call a $\mathbb{B}$ algebra *totally ordered* if its addition induces a total ordering. The next proposition shows that $\mathbb{B}$ algebras which are domains are always totally ordered.

Proposition 3.1.14. *(i) An $\mathbb{B}$-algebra that is a domain is totally ordered.*

(ii) If a $\mathbb{B}$-algebra A is totally ordered then the trivial congruence of A is prime if and only if A is cancellative.

Proof. For (i) let A be a $\mathbb{B}$-algebra which is a domain and $x, y \in A$ two arbitrary elements. We have that

$$(x + y, x)(x + y, y) = (x^2 + y^2 + xy, x^2 + y^2 + xy) \in \Delta.$$

Since the trivial congruence is prime either $(x + y, x) \in \Delta$ or $(x + y, y) \in \Delta$, so indeed at least one of $x \geq y$ or $y \geq x$ hold. For (ii) one direction is clear by (iv) of Proposition 3.1.13. For the other direction assume that A is a totally ordered and cancellative. Let α, β be two pairs satisfying $\alpha\beta \in \Delta$. We can assume that $\alpha_1 \geq \alpha_2$, $\beta_1 \geq \beta_2$ and $\alpha_1\beta_2 \geq \alpha_2\beta_1$. Now we have that

$$\alpha\beta = (\alpha_1\beta_1 + \alpha_2\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1) = (\alpha_1\beta_1, \alpha_1\beta_2) \in \Delta.$$

Then since A is cancellative either $\beta \in \Delta$ or $(\alpha_1, 0) \in \Delta$ which, by $\alpha_1 \geq \alpha_2$ implies $\alpha_1 = \alpha_2 = 0$ so $\alpha \in \Delta$. □

A congruence I for which A/I is cancellative will be called *quotient cancellative* or *QC* for short. The main result of this section shows that QC congruences are prime if and only if they are irreducible.

Lemma 3.1.15. *Let A be a cancellative $\mathbb{B}$-algebra, and $\alpha \in A \times A$ a pair. If for some integer $n > 0$ we have $\alpha^n \in \Delta$ then $\alpha \in \Delta$.*

Proof. First let us assume $\alpha^2 \in \Delta$. It follows that $\alpha_1^2 + \alpha_2^2 = \alpha_1\alpha_2$, and then

$$\alpha_1^2\alpha_2 = \alpha_1^3 + \alpha_1\alpha_2^2 \geq \alpha_1\alpha_2^2$$

and similarly $\alpha_1\alpha_2^2 \geq \alpha_1^2\alpha_2$ so we have that $\alpha_1^2\alpha_2 = \alpha_1\alpha_2^2$. Now by cancellativity either α_1 or α_2 is 0 but then since $\alpha^2 = 0$ both are 0, or neither is 0 and then after dividing by $\alpha_1\alpha_2$ we obtain $\alpha_1 = \alpha_2$.

Now in the general case if $\alpha^n \in \Delta$ then every power of α greater than n is in Δ, in particular for some k we have $\alpha^{2^k} \in \Delta$ and we are done by applying the first half of the argument. □

Lemma 3.1.16. *Let A be a cancellative $\mathbb{B}$-algebra, then for any pair $\alpha \in A \times A$ the set $Ann_A(\alpha)$ is a congruence.*

Proof. If $\alpha \in \Delta$ then $Ann_A(\alpha) = A \times A$, which is a congruence. Assume now that $\alpha \notin \Delta$. The axioms (C1),(C2),(C4) and (C5) are easy to verify. For transitivity consider some pairs (x, y) and (y, z) for which we have $(x, y)\alpha \in \Delta$ and $(y, z)\alpha \in \Delta$. Since $\alpha \notin \Delta$ and A is cancellative we can assume that none of x, y, z is 0. We will show that

$$\beta := (y + z, 0)(x, z)\alpha = ((y + z)x, (y + z)z)\alpha \in \Delta$$

and since $y + z$ non zero this will imply $(x, z)\alpha \in \Delta$. Expanding the above we obtain:

$$(\beta_1, \beta_2) = ((y + z)x, (y + z)z)(\alpha_1, \alpha_2) = (yx\alpha_1 + yz\alpha_2 + zx\alpha_1 + z^2\alpha_2, yx\alpha_2 + yz\alpha_1 + zx\alpha_2 + z^2\alpha_1)$$

By symmetry it suffices to show that $\beta_1 \geq \beta_2$ (with respect to the ordering that comes from the idempotent addition). We have that $\beta_1 \geq z(y\alpha_2 + x\alpha_1)$ and since $(x, y)\alpha \in \Delta$ we obtain

$$\beta_1 = yx\alpha_1 + yz\alpha_2 + zx\alpha_1 + z^2\alpha_2 + zx\alpha_2 + zy\alpha_1$$

Now we have $z(z\alpha_2 + y\alpha_1)$ amongst the terms, using $(y, z)\alpha \in \Delta$ we get:

$$\beta_1 = yx\alpha_1 + yz\alpha_2 + zx\alpha_1 + z^2\alpha_2 + zx\alpha_2 + zy\alpha_1 + z^2\alpha_1 + zy\alpha_2$$

We obtained $\beta_1 \geq x(y\alpha_1 + z\alpha_2)$, using $(y, z)\alpha \in \Delta$ again we get:

$$\beta_1 = yx\alpha_1 + yz\alpha_2 + zx\alpha_1 + z^2\alpha_2 + zx\alpha_2 + zy\alpha_1 + z^2\alpha_1 + zy\alpha_2 + xz\alpha_1 + xy\alpha_2$$

and finally from $\beta_1 \geq z(x\alpha_1 + y\beta_2)$ and $(x, y)\alpha \in \Delta$ we obtain:

$$\beta_1 = yx\alpha_1 + yz\alpha_2 + zx\alpha_1 + z^2\alpha_2 + zx\alpha_2 + zy\alpha_1 + z^2\alpha_1 + zy\alpha_2 + xz\alpha_1 + xy\alpha_2 + zy\alpha_1 + zx\alpha_2$$

which is indeed bigger than β_2, which is the sum of the 5th, 7th, 10th and 11th terms. Hence $Ann_A(\alpha)$ is a congruence. □

Theorem 3.1.17. *Let A be a $\mathbb{B}$-algebra. A congruence I is prime if and only if it is QC and irreducible.*

Proof. It follows from Proposition 3.1.11 and Proposition 3.1.13 that prime congruences are QC and irreducible. For the other direction, taking the quotient by I, we can assume that $I = \Delta$ is QC and irreducible (so A itself is cancellative). Note that this can be done because all three properties depend on the quotient of the congruence. If Δ is not prime there exists an element $\alpha \notin \Delta$ such that $Ann_A(\alpha) \neq \Delta$. By the previous lemma $Ann_A(\alpha)$ is a congruence. Let $Q = \bigcap_{\beta \in Ann_A(\alpha)} Ann_A(\beta)$. Q is a congruence (as it is an intersection of congruences), and since $\alpha \in Q$ we have $\Delta \subsetneq Q$. Clearly $Ann_A(\alpha)Q = \Delta$, we claim that $Ann_A(\alpha) \cap Q = \Delta$. Otherwise suppose that $\beta \in (Ann_A(\alpha) \cap Q) \setminus \Delta$, since $Ann_A(\alpha)Q = \Delta$ we have that $\beta^2 \in \Delta$, and then by Lemma 3.1.15 we have $\beta \in \Delta$ completing the proof. □

3.2 Radicals of congruences

Our next objective is to establish the notion of radicals of congruences and provide a similar algebraic description to the one in ring theory.

Definition 3.2.1. The *radical* of a congruence I is the intersection of all prime congruences containing I. It is denoted by $Rad(I)$. A congruence I is called a *radical congruence* if $Rad(I) = I$.

Let us introduce the following notation: for a pair α, let $\alpha^* = (\alpha_1 + \alpha_2, 0)$. It is easy to verify the following proposition:

Proposition 3.2.2. *Let $\alpha, \beta \in A$ pairs from the $\mathbb{B}$-algebra A,*

(i) $(\alpha\beta)^* = \alpha^*\beta^*$

(ii) $((\alpha\beta)^*)^k = ((\alpha\beta)^k)^*$

(iii) If $\alpha^* \in \Delta$ then $\alpha \in \Delta$.

Now we will define a property for pairs in $A \times A$ that is analogous to nilpotency from ring theory. The aim of this section is to show that the pairs contained in every prime congruence are precisely the nilpotent ones. A natural first guess would be to define the pair α to be nilpotent if $\alpha^n \in \Delta$ for some n. Indeed, in the case of commutative rings, one could characterize the congruence with kernel the nilradical in this fashion. However as shown by the following example these pairs do not even form a congruence in the case of $\mathbb{B}$-algebras:

Example 3.2.3. In the three variable polynomial semiring $\mathbb{B}[x_1, x_2, x_3]$ take the congruence $I = \langle (x_1, x_2)^2, (x_2, x_3)^2 \rangle$. Since $(x_1, x_2)^2 = (x_1^2 + x_2^2, x_1x_2)$ and $(x_2, x_3)^2 = (x_2^2 + x_3^2, x_2x_3)$ one easily verifies that any pair in $I \setminus \Delta$ will need to contain a monomial divisible by x_2 on both sides, hence we have $(x_1, x_3)^k \notin I$ for any $k > 0$. It follows that in the quotient $\mathbb{B}[x_1, x_2, x_3]/I$ the pairs α that satisfy $\alpha^k \in \Delta$ for some k do not form a congruence, since otherwise (x_1, x_3) would have to be amongst them by transitivity.

Looking for a parallel with congruences in commutative algebra, we arrive at the following easy observation. If I is an ideal, $Rad(I)$ its radical and C_I, $C_{Rad(I)}$ be the corresponding congruences (with kernels I and $Rad(I)$ respectively), then we have $(a, b) \in C_{Rad(I)}$ if and only if for a large enough n $(a, b)^n \in C_I$, where $(a, b)^n$ denotes the twisted n-th power. This follows from $(a, b)^n \in C_I \Leftrightarrow ((a - b)^n, 0) \in C_I$. For semirings the situation is somewhat more complicated, as illustrated by the following example.

Example 3.2.4. Consider the congruence $C = \langle (x^2, y^2) \rangle$ in $\mathbb{T}[x, y]$. Let P be a prime congruence lying over C then we have

$$(x^2 + xy, y^2 + xy) \in P, \text{ hence}$$

$$(x + y, 0)(x, y) \in P$$

It follows that either $(x, y) \in P$ or $(x+y, 0) \in P$. On the other hand if $(x+y, 0) \in P$ then $(x, 0) \in P$ and $(y, 0) \in P$ so again $(x, y) \in P$. It follows that $(x, y) \in Rad(C)$. However $(x, y)^n$ is not in C for any n.

To remedy these problems we will introduce some formulas, motivated by the above example, called generalized powers of pairs that will turn out to have the desired properties.

Definition 3.2.5. For a pair α from the $\mathbb{B}$-algebra A, the *generalized powers* of α are the pairs of the form $(\alpha^{*k} + (c, 0))\alpha^l$ where k, l are non-negative integers, and $c \in A$ an arbitrary element. The set of generalized powers of α is denoted by $GP(\alpha)$. A pair α is called *nilpotent* if $GP(\alpha) \cap \Delta \neq \emptyset$.

Proposition 3.2.6. *For an arbitrary pair α the set $GP(\alpha)$ is closed under twisted product. Moreover if $\beta \in GP(\alpha)$ then $GP(\beta) \subseteq GP(\alpha)$.*

Proof. Both claims follow directly from the definition and Proposition 3.2.2. □

One can immediately show the following:

Proposition 3.2.7. *The nilpotent pairs are contained in every prime congruence.*

Proof. Indeed if $(\alpha^{*k}+(c,0))\alpha^l \in \Delta$ then for any prime congruence P we have that $(\alpha^{*k}+(c,0))\alpha^l \in P$, which implies that either $\alpha \in P$ or $(\alpha^{*k}+(c,0)) \in P$. Moreover if $(\alpha^{*k}+(c,0)) \in P$ then by (ii) in Proposition 3.1.4 we have that $\alpha^{*k} \in P$ and by Proposition 3.2.2 $\alpha^* = (\alpha_1+\alpha_2, 0) \in P$, now applying (i) from Proposition 3.1.4 we get that $(\alpha_1, 0) \in P$ and $(\alpha_2, 0) \in P$ so $\alpha \in P$. □

Now we prepare to show that the reverse implication holds as well. We need the following two lemmas:

Lemma 3.2.8. *Let $x \in A$ be an arbitrary element and $I = \langle (x,0) \rangle$. Then $(y,z) \in I$ if and only if there exist an $r \in A$ such that $y + rx = z + rx$.*

Proof. Let J be the set of pairs (y,z) such that there exist an $r \in A$ such that $y+rx = z+rx$. Clearly $(x,0) \in J$ and $J \subseteq I$, so it is enough to show that J is a congruence. C1 and C2 hold trivially. For C3 assume that $y+rx = z+rx$ and $z+sx = v+sx$, then we have $y+(r+s)x = z+(r+s)x = v+(r+s)x$ giving us $(y,v) \in J$. For C4 and C5 assume that $y+rx = z+rx$ and $v+rx = w+rx$ then we have $y+v+(r+s)x = v+w+(r+s)x$ and $yv+(vr+zs)x = zv+(vr+zs)x = zw+(vr+zs)x$ showing that both conditions hold. □

Lemma 3.2.9. *If for some $c, x \in A$ and a pair α from A we have that*

$$(\alpha^* + (c,0))\alpha \in \langle (x,0) \rangle \cap Ann(x)$$

then there exists a $b \in A$ such that $(\alpha^{*3} + (b,0))\alpha \in \Delta$.

Proof. Since $(\alpha^* + (c,0))\alpha \in \langle (x,0) \rangle$ by Lemma 3.2.8 we have that for some $r \in A$

$$\alpha_1^2 + \alpha_1\alpha_2 + c\alpha_1 + rx = \alpha_2^2 + \alpha_1\alpha_2 + c\alpha_2 + rx$$

Let $y = rx$. By $(\alpha^* + (c,0))\alpha \in Ann(x)$ we have that

$$y(\alpha_1^2 + \alpha_1\alpha_2 + c\alpha_1) = y(\alpha_2^2 + \alpha_1\alpha_2 + c\alpha_2).$$

Set $b = y(\alpha_1 + \alpha_2 + c) + c(\alpha_1 + \alpha_2)^2$, and $\beta = (\alpha^{*3} + (b,0))\alpha$. After expanding we get:

$$\beta_1 = \sum_{i=1}^{4} \alpha_1^i \alpha_2^{(4-i)} + y(\alpha_1^2 + \alpha_1\alpha_2 + c\alpha_1) + c(\sum_{i=1}^{3} \alpha_1^i \alpha_2^{(3-i)})$$

$$\beta_2 = \sum_{i=1}^{4} \alpha_2^i \alpha_1^{(4-i)} + y(\alpha_2^2 + \alpha_1\alpha_2 + c\alpha_2) + c(\sum_{i=1}^{3} \alpha_2^i \alpha_1^{(3-i)})$$

The terms appearing in β_2 but not in β_1 are α_2^4, $y\alpha_2^2$, $yc\alpha_2$, $c\alpha_2^3$. However we have:

$$\beta_1 \geq y(\alpha_1^2 + \alpha_1\alpha_2 + c\alpha_1) = y(\alpha_2^2 + \alpha_1\alpha_2 + c\alpha_2) \geq y\alpha_2^2 + yc\alpha_2$$

It follows that

$$\beta_2 \geq \alpha_2^2(\alpha_1^2 + \alpha_1\alpha_2 + c\alpha_1 + y) = \alpha_2^2(\alpha_2^2 + \alpha_1\alpha_2 + c\alpha_2 + y) \geq \alpha_2^4 + c\alpha_2^3$$

showing us $\beta_1 \geq \beta_2$ and by symmetry $\beta_1 = \beta_2$, so indeed $\beta \in \Delta$. □

We are ready to prove:

Theorem 3.2.10. *For any congruence I of a $\mathbb{B}$-algebra A, we have that*

$$Rad(I) = \{\alpha \mid GP(\alpha) \cap I \neq \emptyset\}.$$

In particular the intersection of every prime congruence of A is precisely the set of nilpotent pairs.

Proof. Note that the intersection of all prime congruences is $Rad(\Delta)$. We can reduce to the case $I = \Delta$ after considering the quotient A/I. Proposition 3.2.7 tells us that the nilpotent elements are contained in $Rad(\Delta)$, for the other direction we have to show that for a non-nilpotent pair α there is a prime congruence P such that $\alpha \notin P$. We have that $GP(\alpha) \cap \Delta = \emptyset$. By Zorn's lemma there is a congruence J that is maximal amongst the congruences that are disjoint from $GP(\alpha)$. If J is prime we are done. Assume J is not prime, we first show that J is irreducible. Assume the contrary $J = K \cap L$ for some congruences $J \subsetneq K, L$. Then the maximality of J implies that there exists a $\beta \in K \cap GP(\alpha)$ and a $\gamma \in L \cap GP(\alpha)$, but then $\beta\gamma \in L \cap K \cap GP(\alpha) = J \cap GP(\alpha)$ a contradiction. So J is not prime but irreducible, then it follows from Theorem 3.1.17 that J is not QC. Thus there exists a non-zero $x \in A/J$ such that $Ann_{A/J}(x) \supset \Delta_{A/J}$. Let K be the congruence generated by $(x, 0)$ in A/J. Again by maximality, we have that every non-trivial congruence in A/J contains some element of $GP(\alpha)$, so in particular for some k, l, c we have an element $(\alpha^{*k} + (c, 0))\alpha^l \in GP(\alpha) \cap Ann_{A/J}(x) \cap K$. After multiplying with some power of α^* or α (depending on which of k or l is larger) we can assume that $k = l$. Now we can apply Lemma 3.2.9 for the pair α^k and the semiring A/J and obtain that for some b we have $(\alpha^{*3k} + (b, 0))\alpha^k \in J$ contradicting $GP(\alpha) \cap J = \emptyset$. □

We conclude this section by a list of corollaries of the above theorem.

Proposition 3.2.11. *QC congruences are radical congruences.*

Proof. By considering the appropriate quotients it is enough to prove the theorem for the case when the congruence is the trivial congruence. We have to show that if for some pair α we have $GP(\alpha) \cap \Delta \neq \emptyset$ then $\alpha \in \Delta$. Suppose that for some k, l we have $(\alpha^{*k} + (c,0))\alpha^l \in \Delta$. Then by cancellativity either $\alpha^l \in \Delta$ and then by Lemma 3.1.15 $\alpha \in \Delta$, or $(\alpha^{*k} + (c,0)) \in \Delta$ and then from Proposition 3.1.4 it follows that $\alpha^{*k} \in \Delta$ which in turn by Proposition 3.2.2 implies that $\alpha^k \in \Delta$, and finally by Lemma 3.1.15 that $\alpha \in \Delta$. □

Let us denote by $\overline{Ann}_A(\alpha)$ the set $\{\beta \mid GP(\alpha\beta) \cap \Delta \neq \emptyset\}$.

Proposition 3.2.12. *Let A be an arbitrary $\mathbb{B}$-algebra and $\alpha \in A \times A$ a pair.*

(i) $\overline{Ann}_A(\alpha)$ is the intersection of all prime congruences not containing α (where by empty intersection we mean the full set $A \times A$), in particular $\overline{Ann}_A(\alpha)$ is a congruence.

(ii) If Δ is a radical congruence then $Ann_A(\alpha) = \overline{Ann}_A(\alpha)$, in particular $Ann_A(\alpha)$ is a congruence.

Proof. First let $\beta \in \overline{Ann}_A(\alpha)$. Then by Theorem 3.2.10, we have that $\alpha\beta \in Rad(\Delta) = \bigcap_{P\ prime} P$, so by the prime property every prime that does not contain α needs to contain β. For the other direction let β be an element of every prime congruence that does not contain α, then $\alpha\beta$ is contained in every prime and by Theorem 3.2.10 $GP(\alpha\beta) \cap \Delta \neq \emptyset$. The second half of the statement follows from the fact that if Δ is a radical congruence then $GP(\alpha\beta) \cap \Delta \neq \emptyset$ implies $\alpha\beta \in \Delta$. □

While it might appear that Proposition 3.2.12 provides a simpler proof for Lemma 3.1.16 and Theorem 3.1.17, but we remind the reader that Theorem 3.1.17 was used in the proof of Theorem 3.2.10 which in turn we used to prove Proposition 3.2.12.

Proposition 3.2.13. *A congruence is prime if and only if it is radical and irreducible.*

Proof. Prime congruences are radical by definition and irreducible by Proposition 3.1.11. For the other direction we can argue the same way as in the proof of Theorem 3.1.17, except that this time $\beta^2 \in \Delta$ implies $\beta \in \Delta$ simply by the definition of a radical congruence. □

3.3 Semialgebras satisfying the ACC

While most of the algebras in this thesis do not satisfy the ascending chain condition (ACC) for congruences, we make a few remarks about the ones that do satisfy it. Firstly, we have the following statement from ring theory that holds in this setting. The argument for it is essentially the same as in the classical case.

Proposition 3.3.1. *Let A be a $\mathbb{B}$-algebra with no infinite ascending chain of radical congruences. Then over every congruence there are finitely many minimal primes.*

Proof. The primes lying over a congruence I are the same as the primes lying over $Rad(I)$, so it is enough to prove the statement for radical congruences. Assume that there are radical congruences of A with infinitely many minimal primes lying over them, and let J be a maximal congruence amongst these. Since J is not prime then by Proposition 3.2.13 it is the intersection of two strictly larger congruences K and L. Then every prime containing J contains at least one of K and L so the minimal primes lying over J are amongst those that are minimal over K or L and by the maximality of J there is only finitely many of these. □

One can define primary congruences in the following way:

Definition 3.3.2. We will call a congruence I of a $\mathbb{B}$-algebra A primary if $\{\alpha \mid \exists \beta \notin I : \alpha\beta \in I\} \subseteq Rad(I)$.

As one would expect this class satisfies the following property:

Proposition 3.3.3. *The radical of a primary congruence is a prime congruence.*

Proof. Let Q be a primary congruence, assume that $Rad(Q)$ is not prime. Then we have $\alpha, \beta \notin Rad(Q)$ such that $\alpha\beta \in Rad(Q)$. Then for some k, l we have $((\alpha\beta)^{*k} + (c, 0))(\alpha\beta)^l \in Q$. Now since $GP(\alpha^l) \subseteq GP(\alpha)$, neither α^l nor β^l can be in $Rad(Q)$ so by the primary property we have that $((\alpha\beta)^{*k} + (c, 0)) \in Q$ implying $(\alpha\beta)^{*k} \in Q$. Since $(\alpha\beta)^{*k} = (\alpha^*)^k(\beta^*)^k$, this means that at least one of α^*, β^* is nilpotent in the quotient by Q, but then since $GP(\alpha^*) \subseteq GP(\alpha)$ we have that α or β is nilpotent, a contradiction. □

Unfortunately, there is no general analogue of primary decomposition from commutative algebra. It is easy to show an example of an irreducible congruence that is not primary in a semiring that satisfies the ACC.

Example 3.3.4. Consider the 4-element $\mathbb{B}$-algebra A, with set of elements $\{1, 0, x, y\}$ satisfying the relations $\{1 + x = 1, x + y = x, x^2 = x, xy = 0, y^2 = 0\}$. It is easy to check that the 3 non-trivial proper congruences of this algebra are $I_1 = \{(0, y)\}$ $I_2 = \{(0, y), (0, x)\}$ $I_3 = \{(0, y), (1, x)\}$. We see that $I_1 \subseteq I_2, I_3$ so Δ is irreducible. $A/I_2 \cong \mathbb{B}$ and $A/I_3 \cong \mathbb{B}$ so I_2 and I_3 are prime congruences. Also we have that $(1,x)(x,0)=(x,x)\in\Delta$, so neither I_1 nor the trivial congruence are prime. It follows that $Rad(\Delta)=I_2\cap I_3=I_1$ and $(1,x)\notin Rad(\Delta)$ so Δ is irreducible but not primary. Also note that $Rad(\Delta)$ in this case is not prime so even if one changes the notion of primary congruences, as long as we require the radical of primaries to be primes this algebra would provide a counterexample to primary decomposition.

4

Dimension Theory

Using the definition of prime congruence proposed in the previous chapter we can compute the Krull dimension of a semiring analogously to commutative ring theory. In this chapter we prove an important result, namely that if R is an idempotent semiring of finite dimension, then $\dim R[x_1, \dots, x_n] = \dim R[x_1^{\pm 1}, \dots, x_n^{\pm 1}] = \dim R + n$. We note that irreducibility of prime congruences is crucial since without it most structures (e.g. $\mathbb{T}[\boldsymbol{x}]$) will contain infinitely long chains of congruences with cancellative quotients.

4.1 Infinite chains of QC congruences

We begin my making a remark justifying our choice for definition a prime congruence in view of defining Krull dimension.

Remark 4.1.1. The heuristics for defining primes the way we do is that for a commutative ring R a congruence $C \subset R \times R$ is prime in our sense if and only if its kernel is a prime ideal in the usual sense. In the previous chapter we saw that it is also easy to deduce from the definition that every prime congruence is QC (or equivalently every domain is cancellative) and irreducible. The converse is also true - but not obvious: in Theorem 3.1.17 it was shown that a congruence of a $\mathbb{B}$-algebra is prime if and only if it is QC and irreducible. The key difference from ring theory (where the class of QC and prime congruences coincide) is that a QC congruence does not need to be irreducible and - as we will see at the end of this section - there are typically much more QC congruences than primes. To avoid possible confusion we point out that our terminology differs from that of [PR14] and [PR15], where the authors call every cancellative semiring a domain.

We mentioned in Remark 4.1.1 that QC congruences do not need to be irreducible. Indeed one can find several examples of such congruences by considering the following proposition:

Proposition 4.1.2. *Let P_i denote the elements of a (possibly infinite) set of prime congruences with trivial kernels in an $\mathbb{B}$-algebra A. Then $\bigcap P_i$ is a QC congruence.*

Proof. Assume $(xa, xb) \in \bigcap P_i$ for some $x, a, b \in A$ and $x \neq 0$. Then $(xa, xb) = (x, 0)(a, b) \in P_i$ for every i. By the assumptions $(x, 0) \notin P_i$ for any i, hence the prime property implies that $(a, b) \in \bigcap P_i$. □

Finally we show that the two variable polynomial (or Laurent polynomial) semiring over any $\mathbb{B}$-algebra contains an infinite ascending chain of QC congruences, hence the class of QC congruences - without further restrictions - does not yield an interesting notion of Krull-dimension.

Proposition 4.1.3. *For a $\mathbb{B}$-algebra A the semirings $A[x, y]$ and $A[x^{\pm 1}, y^{\pm 1}]$ contain infinite ascending chains of QC congruences.*

Proof. By Proposition 3.1.10, $\mathbb{B}$ is a quotient of A, hence it is enough to prove the statement for the case $A = \mathbb{B}$. We will see in the next chapter that to a non-zero real vector $v \in \mathbb{R}^2$ one can assign a (minimal) prime P_v in $\mathbb{B}[x, y]$ or $\mathbb{B}[x^{\pm 1}, y^{\pm 1}]$ which is generated by the set of pairs

$$\{(x^{n_1}y^{n_2} + x^{m_1}y^{m_2}, x^{n_1}y^{n_2}) \mid v_1n_1 + v_2n_2 \geq v_1m_1 + v_2m_2\}.$$

In other words one takes a (possibly not complete) monomial order by scalar multiplying exponent vectors with a fixed v, and the congruence P_v identifies each polynomial with its leading term. Set $C_n = \bigcap_{k \geq n} P_{(k,1)}$. We claim that $C_1 \subset C_2 \subset \dots$ is an infinite ascending chain of congruences with cancellative quotients. Indeed they are QC by Proposition 4.1.2 and are contained in each other by definition. Moreover the containments are strict since $(x + y^j, x) \in P_k$ if and only if $k \geq j$. □

4.2 Dimension of Laurent polynomial semiring with coefficients in an idempotent semifield

We will first determine the dimension of the polynomial and Laurent polynomial semiring with coefficients in a semifield.

We begin by showing that the dimension of the polynomial or Laurent polynomial semirings over a finite dimensional $\mathbb{B}$-algebra is strictly bigger than the dimension of the underlying $\mathbb{B}$-algebra.

Proposition 4.2.1. *Let A be a $\mathbb{B}$-algebra of finite Krull dimension, then* $\dim A[y^{\pm 1}] \geq \dim A + 1$ *and* $\dim A[y] \geq \dim A + 1$*.*

Proof. First assume A is a domain. By Proposition 3.1.14 it is totally ordered with respect to the order coming from addition. Consider the following total ordering on the set of monomials of $A[y^{\pm 1}]$. Let $a_1 y^{n_1}$ and $a_2 y^{n_2}$ be two monomials, then $a_1 y^{n_1} > a_2 y^{n_2}$ if $n_1 > n_2$ or if $n_1 = n_2$ and $a_1 > a_2$. Since A is a domain we can always compare the coefficients. This ordering is compatible with the multiplication on $A[y^{\pm 1}]$.

Consider the congruence generated by $(b + c, c)$, when $c \geq b$, where b, c are monomials of $A[y^{\pm 1}]$. Denote by D the quotient of $A[y^{\pm 1}]$ by this congruence and let

$$\phi : A[y^{\pm 1}] \to D,$$

be the quotient map. Note that D is a domain by Proposition 3.1.14 because it is totally ordered by construction and is cancellative. The kernel of ϕ is a prime congruence, hence $\dim A[y^{\pm 1}] \geq \dim D$. Now consider an evaluation morphism

$$\psi : D \to A, \; y \mapsto 1.$$

Note that $D/\ker \psi = A$, hence $\ker \psi$ is a non-trivial prime congruence of D and thus $\dim D > \dim A$. Hence $\dim A[y^{\pm 1}] \geq \dim A + 1$.

If A is not a domain, then consider a prime $\mathfrak{p}$ which is part of a maximal chain for A. Note that $A/\mathfrak{p}$ is a domain since $\mathfrak{p}$ is prime and $\dim A/\mathfrak{p} = \dim A$. Since $(A/\mathfrak{p})(y)$ is a quotient of $A[y^{\pm 1}]$ we have $\dim A[y^{\pm 1}] \geq \dim(A/\mathfrak{p})(y)$, thus $\dim A[y^{\pm 1}] \geq \dim A + 1$ follows from the first part of the proof. The proof for the case of the polynomial semiring $A[y]$ is essentially the same. □

One can immediately obtain the following:

Proposition 4.2.2. *If A is a $\mathbb{B}$-algebra and* $\dim A[y] = 2$ *(or* $\dim A[y^{\pm 1}] = 2$*) then* $\dim A = 1$*.*

Proof. By Proposition 4.2.1 $\dim A[y^{\pm 1}] > \dim A$ (resp. $\dim A[y] > \dim A$). Thus $\dim A = 0$ or 1. If $\dim A = 0$ then by Proposition 3.1.10 $A/P = \mathbb{B}$ for any prime P of A. Hence any strictly increasing chain of primes in $A[y^{\pm 1}]$ maps to a strictly increasing chain of primes in $\mathbb{B}[y^{\pm 1}]$, and by Proposition 5.1.7 (ii) we have $\dim A[y^{\pm 1}] = \dim \mathbb{B}[y^{\pm 1}] = 1$. □

Next, we show that chains of prime congruences of $A[y^{\pm 1}]$ in which all primes have the same kernel can stabilize at most once when restricted to A. We will need the following two simple lemmas:

Lemma 4.2.3. *Let A be a cancellative $\mathbb{B}$-algebra and $a, b, c, d \in A$ such that $a > b$ and $c > d$, then $ac > bd$.*

Proof. Clearly $ac \geq ad \geq bd$. If $ac = bd$, then we have $ac = ad$, and then by cancellativity $c = d$ or $a = 0$ both contradicting our assumptions. □

Lemma 4.2.4. *Let A be a $\mathbb{B}$-algebra and P be a prime congruence in $A \times A$. If $(x^n, y^n) \in P$ then $(x, y) \in P$.*

Proof. Consider A/P, which is a domain since P is prime. Then we have that $x^n = y^n$ in A/P. We want to show that $x = y$. Assume for contradiction that $x \neq y$. Recall that domains are totally ordered so without loss of generality assume that $x > y$. Then after applying Lemma 4.2.3 n times we arrive at a contradiction. □

We are ready to prove:

Lemma 4.2.5. *Let R be a $\mathbb{B}$-algebra and $P_1 \subset P_2 \subseteq P_3 \subset P_4$ prime congruences of $R[y^{\pm 1}]$ (resp. $R[y]$), satisfying $\ker(P_1) = \ker(P_2) = \ker(P_3) = \ker(P_4)$. Then at least one of $P_1|_R \subset P_2|_R$ or $P_3|_R \subset P_4|_R$ holds.*

Proof. By the assumption there exist two pairs,

$$(f_1, g_1) \in P_2 \setminus P_1, \text{ for some } f_1, g_1 \in R[y^{\pm 1}] \ (\textit{resp. } R[y])$$
$$(f_2, g_2) \in P_4 \setminus P_3, \text{ for some } f_2, g_2 \in R[y^{\pm 1}] \ (\textit{resp. } R[y])$$

The quotient by a prime is totally ordered by Proposition 3.1.14, which by the definition of the ordering means that every sum is identified with at least one of its summands. Hence we may assume that f_1, f_2, g_1 and g_2 are monomials and write the following instead:

$$(ay^{k_1}, by^{k_2}) \in P_2 \setminus P_1, \text{ for some } a_1, b_1 \in R$$
$$(cy^{m_1}, dy^{m_2}) \in P_4 \setminus P_3, \text{ for some } a_2, b_2 \in R,$$

By the assumption that the kernels of $P_{1,2,3,4}$ are the same, none of the elements of the above pairs may be in $\ker(P_1) = \cdots = \ker(P_4)$, implying that $a, b, c, d \notin \ker(P_1)$. It also follows that if $y \in \ker(P_1)$ then $k_1 = k_2 = m_1 = m_2 = 0$ and the statement follows from $(a, b) \in P_2 \setminus P_1$ and $(c, d) \in P_4 \setminus P_3$. For the remainder of the proof we assume that $y \notin \ker(P_1)$. Without loss of generality we can assume that $k_1 \geq k_2$ and $m_1 \geq m_2$, and set $k = k_1 - k_2$ and $m = m_1 - m_2$. Since the quotient by a prime is cancellative and y is not in the kernel of any of $P_{1,2,3,4}$ it follows that $(ay^k, b) \in P_2 \setminus P_1$ and $(cy^m, d) \in P_4 \setminus P_3$.

Thus we have,

$$(a^m y^{km}, b^m) \in P_2 \subset P_4$$

$$(c^k y^{km}, d^k) \in P_4$$

Multiplying the first equation with c^k the second with a^m we obtain:

$$(b^m c^k, d^k a^m) \in P_4$$

as $P_3|_R = P_4|_R$ we also have

$$(b^m c^k, d^k a^m) \in P_3$$

Multiplying by y^{km}

$$(b^m c^k y^{km}, d^k a^m y^{km}) \in P_3$$

But we also know that

$$(a^m y^{km}, b^m) \in P_2 \subseteq P_3$$

So from the above two we obtain that

$$(b^m c^k y^{km}, d^k b^m) \in P_3 \tag{4.2.1}$$

Now since $b \notin \ker(P_3)$ we also have that $b^m \in \ker(P_3)$, since P_3 is prime implying that its quotient is cancellative. Thus we obtain:

$$(c^k y^{km}, d^k) \in P_3$$

But then by Lemma 4.2.4

$$(cy^m, d) \in P_3$$

a contradiction.

□

Proposition 4.2.6. *(i) If $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \dots$ is a chain of primes in $R[y^{\pm 1}]$ or $R[y]$ such that the kernel of every $\mathfrak{p}_i$ is the same, then after restricting the chain to A, in $\mathfrak{p}_1|_R \subseteq \mathfrak{p}_2|_R \dots$ equality* *occurs at most once.*

(ii) For an additively idempotent semifield F we have $\dim F[x_1^{\pm 1}, \dots, x_n^{\pm 1}] = \dim F + n$.

Proof. For (i), assume for contradiction that equality occurs at least twice, say $\mathfrak{p}_i|_R = \mathfrak{p}_{i+1}|_R$ and $\mathfrak{p}_j|_R = \mathfrak{p}_{j+1}|_R$ with $i + 1 \leq j$. Then by setting $P_1 = \mathfrak{p}_i$, $P_2 = \mathfrak{p}_{i+1}$, $P_3 = \mathfrak{p}_j$ and $P_4 = \mathfrak{p}_{j+1}$ we arrive at contradiction with Lemma 4.2.5. (ii) follows by induction from (i) and Proposition 3.1.5 which asserts that in $F[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ the kernel of every congruence is trivial. □

4.3 Dimension of polynomial semiring with coefficients in an idempotent semiring

We will prove the general result by reducing to the previous case. We will prove the statement first in the case when the coefficients of the polynomial or Laurent polynomial semiring lie in a domain. Then we recall that the quotient of A by a prime congruence P is a domain and that we can relate the dimension of the quotient A/P to the dimension of the original semiring A.

We recall that a cancellative semiring R embeds into its semifield of fractions $\mathrm{Frac}(R)$. The elements of $\mathrm{Frac}(R)$ are the equivalence classes in $R \times (R \setminus \{0\})$ of the relation $(r_1, s_1) \sim (r_2, s_2) \Leftrightarrow r_1 s_2 = r_2 s_1$, with operations $(r_1, s_1) + (r_2, s_2) = (r_1 s_2 + r_2 s_1, s_1 s_2)$, $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$. As usual for $(r, s) \in \mathrm{Frac}(R)$ we will write $\frac{r}{s}$. We refer to [Go99] for the details of this construction.

We would like to point out that part (i) of Proposition 4.3.2 is essentially the same as Lemma 2.4.4 of [PR15] and both of parts (i) and (ii) are likely well-known. We provide a short proof for the convenience of the reader. Also, note that Proposition 4.3.2 is not specific to the additively idempotent case.

Lemma 4.3.1. *Let F be a semifield. Let $C \subseteq F \times F$ be symmetric and reflexive and closed under addition and multiplication, that is for $(a_1, b_1), (a_2, b_2) \in C$ we have that $(a_1 + a_2, b_1 + b_2) \in C$ and $(a_1 a_2, b_1 b_2) \in C$. Then C is a congruence.*

Proof. We only need to show that C is transitive. Assume that $(a, b), (b, c) \in C$. If $b = 0$, then $(a + 0, 0 + c) = (a, c) \in C$. If $b \neq 0$ then $(b^{-1}, b^{-1}) \in C$ and $(ab, bc) \in C$, and after multiplying it follows that $(a, c) \in C$. □

Proposition 4.3.2. *Let R be a cancellative semiring. For a congruence C of R denote by $\langle C \rangle_{Frac(R)}$ the congruence generated by C in Frac(R).*

(i) $(a,b) \in \langle C\rangle_{Frac(R)}$ *if and only if there is an* $s \in R\setminus\{0\}$ *such that* $(sa,sb) \in C$. *In particular* $\langle C\rangle_{Frac(R)}$ *is proper if and only if* $\ker(C) = \{0\}$.

(ii) If C *is a QC congruence of* R *with* $\ker(C) = \{0\}$ *then* $\langle C\rangle_{Frac(R)}|_R = C$ *and for any congruence* $\mathfrak{C}$ *of Frac*(R) *we have* $\langle \mathfrak{C}|_R\rangle_{Frac(R)} = \mathfrak{C}$.

(iii) If C *is a QC congruence of* R *with* $\ker(C) = \{0\}$, *then* C *is prime if and only if* $\langle C\rangle_{Frac(R)}$ *is prime. If* $\mathfrak{C}$ *is a congruence of Frac*(R) *then* $\mathfrak{C}$ *is prime if and only if* $\mathfrak{C}|_R$ *is prime.*

Proof. For (i) set

$$C' = \{(a,b) \in \mathrm{Frac}(R) \times \mathrm{Frac}(R) |\, \exists s \in R\setminus\{0\} :\ (sa,sb) \in C\}.$$

Since every $s \in R\setminus\{0\}$ has a multiplicative inverse in Frac(R) it is clear that $C \subseteq C' \subseteq \langle C\rangle_{\mathrm{Frac}(R)}$. Hence one only needs to see that C' is a congruence. If $s_1, s_2 \in R\setminus\{0\}$ is such that $(s_1a_1, s_1b_1) \in C$ and $(s_2a_2, s_2b_2) \in C$ for some $(a_1,b_1),(a_2,b_2) \in \mathrm{Frac}(R)\times\mathrm{Frac}(R)$ then we have

$$(s_1s_2(a_1+a_2), s_1s_2(b_1+b_2)) \in C$$

and

$$(s_1s_2(a_1a_2), s_1s_2(b_1b_2)) \in C$$

showing that C' is closed under addition and multiplication (note that $s_1s_2 \neq 0$ since R is cancellative). Since C' is clearly symmetric and reflexive it follows from Lemma 4.3.1 that C' is indeed a congruence. It follows that $\langle C\rangle_{\mathrm{Frac}(R)}$ is proper if and only if there exists no $s \in R\setminus\{0\}$ such that $(s,0) \in C$ or equivalently if $\ker(C) = \{0\}$.

For (ii) first note that it is immediate from the definition of C' that if C is a QC congruence of R with $\ker(C) = \{0\}$ then $C' \cap R\times R = C$, implying that $\langle C\rangle_{\mathrm{Frac}(R)}|_R = C$. On the other hand if $\mathfrak{C}$ is a congruence of Frac(R) then it is clear that $\langle \mathfrak{C}|_R\rangle_{\mathrm{Frac}(R)} \subseteq \mathfrak{C}$. For the other direction if $(\frac{r_1}{s_1}, \frac{r_2}{s_2}) \in \mathfrak{C}$ then $(r_1s_2, r_2s_1) \in \mathfrak{C}|_R$ implying that $(\frac{r_1}{s_1}, \frac{r_2}{s_2}) \in \langle \mathfrak{C}|_R\rangle_{\mathrm{Frac}(R)}$.

For the first statement of (iii) recall that the restriction of a prime to a subsemiring is always a prime, hence if $\langle C\rangle_{\mathrm{Frac}(R)}$ is a prime congruence, where C is a congruence of R with $\ker(C) = \{0\}$, then $C = \langle C\rangle_{\mathrm{Frac}(R)}|_R$ is also a prime. For the other direction assume that C is a prime of R with $\ker(C) = \{0\}$ and we have a twisted product $(\frac{r_1}{s_1}, \frac{r_2}{s_2})(\frac{r_1'}{s_1'}, \frac{r_2'}{s_2'}) \in \langle C\rangle_{\mathrm{Frac}(R)}$. Then by (i) it follows that $(r_1s_2, r_2s_1)(r_1's_2', r_2's_1') \in C$. Since C is a prime congruence we obtain that one of the factors in the twisted product, say $(r_1 s_2, r_2 s_1)$, has to be in C and thus $(\frac{r_1}{s_1}, \frac{r_2}{s_2}) \in \langle C \rangle_{\mathrm{Frac}(R)}$ showing that $\langle C \rangle_{\mathrm{Frac}(R)}$ is prime. The second statement in (iii) follows from the first statement and (ii). □

We also recall the following well-known statement:

Proposition 4.3.3. *In a semifield every proper congruence is determined by the equivalence class of* 1*.*

Proof. Indeed if C is a proper congruence of a semifield then $\ker(C) = \{0\}$ and $(a, b) \in C$ if and only if $a = b = 0$ or $(a/b, 1) \in C$. □

Next we collect some elementary observations about additively idempotent semifields that are domains which we will need to prove our main result. We point out that an additively idempotent semifield needs not to be a domain in general. If A is a cancellative $\mathbb{B}$-algebra that is not totally ordered then by Proposition 3.1.14 $\mathrm{Frac}(A)$ is an additively idempotent semifield that is not a domain. In the proof of Proposition 4.3.5 we will often use the following trivial but important fact:

Lemma 4.3.4. *Let A be a $\mathbb{B}$-algebra. If $x, y \in A$ both have multiplicative inverses then $x \geq y$ if and only if $1/y \geq 1/x$.*

Proof. $x \geq y$ means $x + y = x$, multiplying both sides by $\frac{1}{xy}$ we get $1/y + 1/x = 1/y$ showing that $1/y \geq 1/x$. □

Proposition 4.3.5. *Let F be an additively idempotent semifield that is a domain.*

(i) Every proper congruence of F is prime.

(ii) The congruences of F form a chain. Moreover if $\dim F$ is finite, then every congruence is principal, i.e. generated by $(1, x)$ for some $x \in F \setminus \{0\}$.

(iii) For $x, y \in F \setminus \{0\}$, we have that $(1, y) \in \langle (1, x) \rangle$ if and only if there exist an $n \in \mathbb{Z}$ such that $1 \leq y \leq x^n$ or $1 \geq y \geq x^n$.

Proof. First note that a proper congruence of any semifield is always cancellative, since if $(ca, cb) \in C$ for $c \neq 0$ then multiplying by c^{-1} we get $(a, b) \in C$. Now (i) follows from Proposition 3.1.14 and the fact that the quotient of a totally ordered $\mathbb{B}$-algebra is also totally ordered.

For (ii) assume that there are two congruences C_1 and C_2 such that $C_1 \not\subseteq C_2$ and $C_2 \not\subseteq C_1$. Then by Proposition 4.3.3 we have $x, y \in F \setminus \{0\}$ such that $(1, x) \in C_1 \setminus C_2$ and $(1, y) \in C_2 \setminus C_1$. By possibly replacing x or y with their multiplicative inverse we may assume that $x, y \geq 1$. Moreover

F is totally ordered, thus without loss of generality we can set $x \geq y$. Now it follows from (ii) of Proposition 3.1.4 that $(1, y) \in C_1$, a contradiction. When $\dim F$ is finite this implies that there is a unique chain of primes $\Delta = P_0 \subset P_1 \cdots \subset P_{\dim F}$ in F. Choosing any $(a, b) \in P_k \setminus P_{k-1}$ we see that $\langle (a/b, 1) \rangle = P_k$ proving the second statement in (ii).

For (iii) set $H \subset F \times F$ to consist of the pair $(0, 0)$ and the pairs $(a, b) \in (F \setminus \{0\}) \times F \setminus \{0\}$ for which exists an $n \in \mathbb{Z}$ such that $1 \leq b/a \leq x^n$ or $1 \geq b/a \geq x^n$. We need to show that $H = \langle (1, x) \rangle$ to prove the claim. Clearly we have $(1, x) \in H$ and by Proposition 3.1.14 we also have that $H \subseteq \langle (1, x) \rangle$ so we only need to show that H is a congruence. Note that if $(y, 1), (z, 1) \in H$ and $y \leq v \leq z$ then we also have $(v, 1) \in H$, moreover that $(a, b) \in H$ if and only if $(1, b/a) \in H$. First we show that if $(a_1, b_1), (a_2, b_2) \in H$ then $(a_1 + a_2, b_1 + b_2) \in H$. Without loss of generality we may assume $a_1 \geq a_2$. If $b_1 \geq b_2$ then $(a_1 + a_2, b_1 + b_2) = (a_1, b_1)$ and the claim is obvious. If $b_2 \geq b_1$ then $(a_1 + a_2, b_1 + b_2) = (a_1, b_2)$, moreover we have $b_2/a_2 \geq b_2/a_1 \geq b_1/a_1$ showing that $(1, b_2/a_1) \in H$, hence $(a_1, b_2) \in H$. To show that H is closed under products let $(a_1, b_1), (a_2, b_2) \in H$ and let n_1, n_2 be integers as in the definition of H. Without loss of generality we can assume $x \geq 1$ and then we have $x^{-(|n_1|+|n_2|)} \leq \frac{a_1 a_2}{b_1 b_2} \leq x^{|n_1|+|n_2|}$, hence $(a_1 a_2, b_1 b_2) \in H$. Finally H is symmetric since $1 \leq b/a \leq x^n$ if and only if $1 \geq a/b \geq x^{-n}$, hence by Lemma 4.3.1 H is a congruence. □

Corollary 4.3.6. *If an $\mathbb{B}$-algebra A is a domain, then the prime congruences of A with trivial kernels form a chain.*

Proof. This follows immediately from Proposition 4.3.2 and (ii) of Proposition 4.3.5. □

Remark 4.3.7. We would like to point out that (iii) of Proposition 4.3.5 can also be deduced from Proposition 4.1.3. in [PR14] and the second statement in (ii) could be recovered from Remark 4.1.8 in [PR14]. We also call the reader's attention to the fact that that kernels in [PR14] refer to the equivalence class of 1 in a congruence and not to the equivalence class of 0 as in the current paper.

Let F be an additively idempotent semifield that is a domain and for $x \in F \setminus \{0\}$ denote by P_x the unique minimal prime containing $(1, x)$. For $x, y \in F \setminus \{0\}$ we will write $x \trianglelefteq_F y$ whenever $x \in P_y$ and $x \diamond_F y$ whenever $P_x = P_y$. Clearly $\diamond$ is an equivalence relation, and when F is finite dimensional the number of its equivalence classes is $\dim F + 1$.

Lemma 4.3.8. *Let A be a $\mathbb{B}$-algebra that is a domain, and $x, y, z \in A \setminus \{0\}$ with $x \trianglelefteq_{Frac(A)} \frac{y}{z}$. Then for any prime congruence P with $x \in \ker(P)$ we also have that at least one of $y \in \ker(P)$ or $z \in \ker(P)$ hold.*

Proof. By (iii) of Proposition 4.3.5 we have that there exist an $n \in \mathbb{Z}$ such that $1 \leq x \leq \frac{y^n}{z^n}$ or $1 \geq x \geq \frac{y^n}{z^n}$ holds in $\mathrm{Frac}(A)$. If $1 \leq x \leq \frac{y^n}{z^n}$ then, by Proposition 3.1.4, $x \in \ker(P)$ implies $1 \in \ker(P)$ contradicting that P is proper. If $1 \geq x \geq \frac{y^n}{z^n}$ with $n \geq 0$ then after multiplying with z^n we obtain $z^n \geq xz^n \geq y^n$. Since $xz^n \in \ker(P)$ by Proposition 3.1.4 we have that $y^n \in ker(P)$. Since P is prime it follows that $y \in \ker(P)$. If $n < 0$ then after multiplying by y^{-n} we obtain that $y^{-n} \geq xy^{-n} \geq z^n$. Since $xy^{-n} \in A$ we have $xy^{-n} \in \ker(P)$ and it follows that $z^n \in \ker(P)$ and thus $z \in \ker(P)$. □

Proposition 4.3.9. *Let A be a $\mathbb{B}$-algebra that is a domain, with $\dim A < \infty$. Then $\dim A = \dim Frac(A)$, in particular the primes of A with a trivial kernel form a chain of maximal length.*

Proof. First it follows immediately from Proposition 4.3.2 that $\dim A \geq \dim \mathrm{Frac}(A)$ since the unique chain of primes in $\mathrm{Frac}(A)$ restricts to a chain of primes in $\dim A$ of the same length. We will prove by induction on $\dim \mathrm{Frac}(A)$. If $\dim \mathrm{Frac}(A) = 0$ then by Proposition 3.1.10 $\mathrm{Frac}(A) \simeq \mathbb{B}$, and since A embeds into $\mathrm{Frac}(A)$ we also have that $A \simeq \mathbb{B}$.

Next we assume that $\dim \mathrm{Frac}(A) = d > 0$ and that the claim holds for all $d' < d$. Let

$$\Delta = P_0 \subset P_1 \subset \cdots \subset P_{\dim A}$$

be a chain of maximal length in A and set $A' = A/P_1$. Clearly $\dim A' = \dim A - 1$. If $\ker(P_1) = \{0\}$ then applying Proposition 4.3.2 we see that P_1 extends to a prime $\langle P_1 \rangle_{\mathrm{Frac}(A)}$ of $\mathrm{Frac}(A)$ and $\dim \mathrm{Frac}(A)/\langle P_1 \rangle_{\mathrm{Frac}(A)} = d - 1$. It follows that $\dim \mathrm{Frac}(A') = d - 1$ and applying the induction hypothesis we obtain $\dim A' = d - 1$, and thus $\dim A = d$.

We are left to deal with the case when $0 \neq x \in \ker(P_1)$. First note that the elements of $\mathrm{Frac}(A')$ can be written as $\frac{[a]}{[b]}$ with $a, b \in A$ and $b \notin \ker(P_1)$, where $[a], [b]$ denote the images of a, b in A'. (Note however that there is no natural map from $\mathrm{Frac}(A)$ to $\mathrm{Frac}(A')$ in this case.) Now it follows from (iii) of Proposition 4.3.5 that for $\frac{[a]}{[b]}, \frac{[c]}{[d]} \in \mathrm{Frac}(A')$, if we have that $\frac{a}{b} \diamond_{\mathrm{Frac}(A)} \frac{c}{d}$ then $\frac{[a]}{[b]} \diamond_{\mathrm{Frac}(A')} \frac{[c]}{[d]}$. Finally it follows from Lemma 4.3.8 that whenever $x \diamond_{\mathrm{Frac}(A)} \frac{a}{b}$ at least one of a or b map to 0 in A', hence $\diamond_{\mathrm{Frac}(A')}$ has strictly less equivalence classes than $\diamond_{\mathrm{Frac}(A)}$. We obtained that $\dim \mathrm{Frac}(A') \leq d - 1$, and hence by the induction hypothesis we have that $\dim A' = \dim \mathrm{Frac}(A')$ and it follows that $\dim A = \dim A' + 1 = d$. □

We are ready to state our main result:

Theorem 4.3.10. *Let A be a $\mathbb{B}$-algebra with $\dim A < \infty$. Then we have that $\dim A[y^{\pm 1}] = \dim A[y] = \dim A + 1$.*

Proof. Let $P_0 \subset P_1 \cdots \subset P_{\dim A[y^{\pm 1}]}$ be a chain of primes of maximal length in $A[y^{\pm 1}]$. By Proposition 4.3.9 we may assume that the congruences P_i/P_0 have trivial kernel in $A[y^{\pm 1}]/P_0$ or equivalently that $\ker(P_0) = \ker(P_i)$ for all $0 \leq i \leq \dim A[y^{\pm 1}]$. Now it follows from (i) of Proposition 4.2.6 that after restricting the chain to A, in $P_0|_A \subseteq P_1|_A \subseteq \ldots$ equality occurs at most once proving that $\dim A + 1 \geq \dim A[y^{\pm 1}]$. Finally by Proposition 4.2.1 we also have that $\dim A + 1 \leq \dim A[y^{\pm 1}]$, proving that $\dim A[y^{\pm 1}] = \dim A + 1$. The equality $\dim A[y] = \dim A + 1$ can be verified by the same argument. □

Remark 4.3.11. In commutative algebra (e.g. [Ei95]), if R is a Noetherian ring of finite dimension then we have that

$$\dim R[x] = \dim R + 1.$$

However, if we consider a non-Noetherian ring S of finite dimension, we have the following inequality for the polynomial ring with coefficients in S

$$\dim S + 1 \leq \dim S[x] \leq 2 \dim S + 1.$$

Furthermore, for any N, $s + 1 \leq N \leq 2s + 1$ one can find a ring S of dimension s, such that $S[x]$ is N-dimensional. For the proof of this claim we refer the reader to [Se54].

5

Prime congruences of polynomial and Laurent polynomial semirings with coefficients in $\mathbb{B}$, $\mathbb{Z}_{max}$, $\mathbb{T}$

Our next goal is to understand the prime congruences of the polynomial and Laurent polynomial rings over the semifields $\mathbb{B}$, $\mathbb{Z}_{max}$ and $\mathbb{T}$. In all of these cases minimal primes turn out to correspond to monomial orderings. Applying a result of Robbiano from [Rob85] that classifies monomial orderings, it can be then shown that every prime congruence of these semirings can be described by a certain defining matrix.

We show that in the considered cases above every congruence there exists a unique chain of primes. We show that the dimension of the quotient by a prime is equal to the number of rows of its defining matrix. As a consequence and in accordance with the results from the previous chapter the dimension of a k-variable polynomial or Laurent polynomial semiring is k over $\mathbb{B}$ and $k+1$ over $\mathbb{T}$ or $\mathbb{Z}_{max}$.

Furthermore using this description of prime congruences we show that two polynomials with coefficients in $\mathbb{B}$ are congruent in every prime if and only if their Newton polytopes are the same. Consequently the quotient of the polynomial algebra over $\mathbb{B}$ by the intersection of all prime congruences (i.e. the radical of the trivial congruence) can be described as the semiring of lattice polytopes with the sum of two polytopes being the convex hull of their union and the product the Minkowski sum. Similar descriptions can be given in all of the other studied cases.

5.1 The prime congruences of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ and $\mathbb{B}[\boldsymbol{x}]$

Throughout this section $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ and $\mathbb{B}[\boldsymbol{x}]$ denote respectively the Laurent polynomial semiring and the polynomial semiring in k variables $\boldsymbol{x} = (x_1, \dots, x_k)$. First we show that the kernel of the primes of these semirings are easy to describe:

Proposition 5.1.1. *(i) For any proper congruence I of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$, we have that $Ker(I) = \{0\}$.*

(ii) For any QC congruence Q of $\mathbb{B}[\boldsymbol{x}]$ we have that $Ker(Q)$ is the polynomial semialgebra generated by a subset of the variables $x_1, \dots, x_k$.

Proof. In both cases by Proposition 3.1.4 we have that the kernel of any congruence is generated by monomials. In the case of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ any monomial has a multiplicative inverse, so if $Ker(I) \neq \{0\}$ then we have $(1, 0) \in Ker(I)$ so I has to be the improper congruence. For (ii) if Q is QC then $(fg, 0) \in Q$ implies that $(f, 0) \in Q$ or $(g, 0) \in Q$, so a monomial is in $Ker(Q)$ if and only if at least one of the variables in that monomial is in $Ker(Q)$. □

So in fact prime congruences of $\mathbb{B}[\boldsymbol{x}]$ with non-zero kernels will correspond to prime congruences of a polynomial semirings in less variables. Next recall that quotients by primes are totally ordered and consider the following proposition:

Proposition 5.1.2. *(i) If Q is a congruence of $\mathbb{B}[\boldsymbol{x}]$ or $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ such that the quotient by Q is totally ordered, then in each equivalence class of Q there is at least one monomial.*

(ii) A congruence P of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ is prime if and only if $\mathbb{B}[\boldsymbol{x}^{\pm 1}]/P$ is totally ordered.

(iii) If Q is a prime congruence of $\mathbb{B}[\boldsymbol{x}]$ with $Ker(Q) = \{0\}$, then $Q = P|_{\mathbb{B}[\boldsymbol{x}]} = P$ for some prime congruence P of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$.

(iv) For a prime P of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ the multiplicative monoid of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]/P$ is isomorphic to a quotient of the additive group $(\mathbb{Z}^k, +)$. For a prime P of $\mathbb{B}[\boldsymbol{x}]$ the multiplicative monoid of $\mathbb{B}[\boldsymbol{x}]/P$ is isomorphic to the restriction of a quotient of the additive group $(\mathbb{Z}^{k'}, +)$ to $(\mathbb{N}^{k'}, +)$, where $k - k' = |\{x_1, \dots, x_k\} \cap Ker(P)|$.

Proof. The first statement follows from the fact that if the quotient is totally ordered, then every polynomial is congruent to any of its monomials that is maximal with respect to the ordering on the quotient. For (ii) consider that every monomial in $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ has a multiplicative inverse, so by (i) we see that the if the quotient by a congruence P is totally ordered then it is a semifield, which is in particular cancellative and then by Proposition 3.1.14 P is prime. For (iii) first note that congruences of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ with totally ordered quotients are determined by the equivalence class of 1. Take a prime congruence Q of $\mathbb{B}[\boldsymbol{x}]$ with $Ker(Q) = \{0\}$, and let P be the congruence of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ with a totally ordered quotient satisfying that for any monomials $m_1, m_2 \in \mathbb{B}[\boldsymbol{x}]$:

$$(1, m_1/m_2) \in P \iff (m_2, m_1) \in Q \text{ and } (1, m_1/m_2 + 1) \in P \iff (m_2, m_1 + m_2) \in Q.$$

Note that while writing a Laurent monomial as quotient of monomials of $\mathbb{B}[\boldsymbol{x}]$ is not done uniquely, the above is still well defined because of the QC property of Q. P is prime since its quotient is totally ordered and cancellative and it is straightforward to check that $P|_{\mathbb{B}[\boldsymbol{x}]} = Q$. (iv) follows from (i),(iii) and Proposition 5.1.1. □

A *group ordering* (resp. *semigroup ordering*) of a group (resp. semigroup) $(G, +)$, is an ordering $\leq$ on the the elements of G satisfying that for any $g_1, g_2 \in G$ with $g_1 \leq g_2$ and an arbitrary $g_3 \in G$ we have $g_1 + g_3 \leq g_2 + g_3$. The previous proposition tells us that to understand the the prime quotients of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ we need to describe the group orderings on the quotients of $(\mathbb{Z}^k, +)$. When we think of $(\mathbb{Z}^k, +)$ (resp. $(\mathbb{N}^k, +)$) as the group (resp. semigroup) of Laurent monomials (resp. monomials) with the usual multiplication their group orderings are called *term orderings*. (Note that in the literature it is sometimes required that the generating variables are larger than the unit under a term ordering, but we do not use this convention). Term orderings are described by a result of Robbiano in [Rob85]:

Proposition 5.1.3. *For every term ordering $\leq$ of the Laurent monomials $\{\boldsymbol{x}^{\boldsymbol{n}} \mid \boldsymbol{n} \in \mathbb{Z}^k\}$ there exist a matrix U with k columns and $l \leq k$ rows, such that $\boldsymbol{x}^{\boldsymbol{n}_1} < \boldsymbol{x}^{\boldsymbol{n}_2}$ if and only if the first non-zero coordinate of $U(\boldsymbol{n}_2 - \boldsymbol{n}_1)$ is positive. Term orderings of the monomials $\{\boldsymbol{x}^{\boldsymbol{n}} \mid \boldsymbol{n} \in \mathbb{N}^k\}$ are restrictions of the orderings on the Laurent monomials.*

We will say that the i-th row of the matrix U is *non-redundant* if there is an integer vector $\boldsymbol{n} \in \mathbb{Z}^k$ such that the first non-zero coordinate of $U\boldsymbol{n}$ is the i-th coordinate. If all of the rows of U are non-redundant we will call it an *admissible* matrix. If U is an admissible matrix for an ordering as in the setting of Proposition 5.1.3, then it will be called a defining matrix of the ordering. It is easy to verify that the defining matrix can always be chosen to have orthonormal rows, and that for an ordering defined by a square matrix there is a unique orthogonal defining matrix.As explained above, term orderings define prime congruences of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ and $\mathbb{B}[\boldsymbol{x}]$, which will be denoted by $P(U)$ and $P[U]$ respectively. One can also consider the $\mathbb{B}$-algebra of Laurent monomials (resp. monomials) whose addition is defined by the term ordering of U, and the surjections from $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ (resp. $\mathbb{B}[\boldsymbol{x}]$)

onto these that map each polynomial to their leading monomial, then $P(U)$ (resp. $P[U]$) are just the kernel of these maps. Note that prime congruences given by term orderings are minimal by (i) of Proposition 5.1.2 since every equivalence class of them contains precisely one monomial.

If an admissible matrix U is the defining matrix of a term ordering then the zero vector is the only integer vector in the kernel of U, since a term ordering is a total ordering of all of the monomials. If U has integer vectors in its kernel, it still gives us a group ordering on the quotient $\mathbb{Z}^k/(Ker(U) \cap \mathbb{Z}^k)$, defined the same way as in Proposition 5.1.3. In this case we will still call U the defining matrix of the ordering on that quotient and denote by $P(U)$ or $P[U]$ the corresponding prime congruences of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ and $\mathbb{B}[\boldsymbol{x}]$. Explicitly speaking, $P(U)$ is generated by the pairs $(\boldsymbol{x}^{\boldsymbol{n}_1} + \boldsymbol{x}^{\boldsymbol{n}_2}, \boldsymbol{x}^{\boldsymbol{n}_2})$ such that either $U(\boldsymbol{n}_2 - \boldsymbol{n}_1) = \mathbf{0}$ or the first non-zero coordinate of $U(\boldsymbol{n}_1 - \boldsymbol{n}_2)$ is positive and $P[U] = P(U)|_{\mathbb{B}[\boldsymbol{x}]}$. We will soon see that every prime congruence of these $\mathbb{B}$-algebras arise this way.

Example 5.1.4. Let $U = \begin{bmatrix} -1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$, that defines the prime $P(U)$ in $\mathbb{B}(x,y,z)$. This matrix defines an ordering on the monomials in $\mathbb{B}(x,y,z)/P(U)$. Consider the monomials $m_1 = x^2y^3z$ and $m_2 = x^3yz^2$. Using the notation of Proposition 5.1.3 we have that $\boldsymbol{n}_1 = \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix}$, $\boldsymbol{n}_2 = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}$ and $U\boldsymbol{n}_1 = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$, $U\boldsymbol{n}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Notice that $U\boldsymbol{n}_1 - U\boldsymbol{n}_2 = \begin{bmatrix} 2 \\ 3 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$, and thus in $\mathbb{B}(x,y,z)/P(U)$ we have that $m_1 > m_2$. Now consider the monomials $m_3 = xy^2z$ and $m_4 = x^2y^2z^2$. Here we have that $U\boldsymbol{n}_3 = U\boldsymbol{n}_4$, that is $\boldsymbol{n}_3 - \boldsymbol{n}_4 \in Ker(U) \cap \mathbb{Z}^k)$ and thus $m_3 = m_4$ in $\mathbb{B}(x,y,z)/P(U)$.

Since the rows of an admissible matrix U are linearly independent its rank $r(U)$ is equal to the number of its rows. For $i \leq r = r(U)$ let us denote by $U(i)$ the matrix that consists of the first i rows of U. Note that if U is admissible then so are all of the $U(i)$. Let us use the convention that $U(0)$ for any U is the "empty matrix" which corresponds to the only group ordering of the one element quotient $\mathbb{Z}^k/\mathbb{Z}^k$ and $P(U(0))$ (resp. $P[U(0)]$) are the maximal congruences of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ (resp. $\mathbb{B}[\boldsymbol{x}]$) that identify every non-zero element with 1. Accordingly we will write $r(U(0)) = 0$. Now we describe the primes lying above a congruence $P(U)$.

Proposition 5.1.5. *Let U be an admissible matrix with k columns. Then every proper congruence of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ containing $P(U)$ is an element of the strictly increasing chain*

$$P(U) = P(U(r(U))) \subset P(U(r(U)-1)) \subset \cdots \subset P((U(0))).$$

In particular every proper congruence of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]/P(U)$ *is prime and dim*$(\mathbb{B}[\boldsymbol{x}^{\pm 1}]/P(U)) = r(U)$.

Proof. The congruences $P(U(i))$ are prime since their quotients are totally ordered and cancellative. Furthermore the chain in the proposition is strictly increasing since the rows of U are non-redundant. Since the $P(U(i))$-s form a finite chain, it is enough to verify that every congruence that is generated by a single pair is one of these, and then it will follow for an arbitrary congruence $P(U) \subseteq I$ that $I = P(U(i))$ where i is the smallest such that $P(U(i))$ can be generated by a pair in I. Note that in a semifield each congruence is determined by the equivalence class of 1, since for any congruence I we have that $(\alpha_1, \alpha_2) \in I \iff (\alpha_1\alpha_2^{-1}, 1) \in I$. Therefore for any congruence $P(U) \subsetneq I$ generated by a single pair we have that $I = \langle (1, \boldsymbol{x}^{\boldsymbol{n}}) \rangle$ for some $\boldsymbol{n} \in \mathbb{Z}^k$ satisfying $\boldsymbol{n} \notin Ker(U)$. Let s be the smallest integer such that for the s-entry of $U\boldsymbol{n}$ we have $(U\boldsymbol{n})[s] \neq 0$, then we have that $(1, \boldsymbol{x}^{\boldsymbol{n}}) \in P(U(s-1))$. Moreover, if $(1, \boldsymbol{x}^{\boldsymbol{n}'}) \in P(U(s-1))$ for some $\boldsymbol{n}'$, then $\forall j < s : \ (U\boldsymbol{n}')[j] = 0$. Then for some $k \in \mathbb{Z}$ with large enough absolute value we have that either $1 \leq \boldsymbol{x}^{\boldsymbol{n}'} \leq \boldsymbol{x}^{k\boldsymbol{n}}$ or $\boldsymbol{x}^{k\boldsymbol{n}} \leq \boldsymbol{x}^{\boldsymbol{n}'} \leq 1$ where $\leq$ is the ordering on the quotient $\mathbb{B}[\boldsymbol{x}^{\pm 1}]/P(U)$. Then by (iii) of Proposition 3.1.4 we have that $(1, \boldsymbol{x}^{\boldsymbol{n}'}) \in I$, so $P(U(s-1)) \subseteq I$ and then $P(U(s-1)) = I$. □

Finally we need the following lemma to prove our main result:

Lemma 5.1.6. *For every prime congruence* Q *of* $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ *we have an admissible matrix* U *such that* $P(U) \subseteq Q$ *and* $Ker(U) \cap \mathbb{Z}^k = \{\boldsymbol{0}\}$.

Proof. Recall that for an admissible matrix U the condition $Ker(U) \cap \mathbb{Z}^k = \{\boldsymbol{0}\}$ is equivalent to saying that U is the defining matrix of a term ordering. Intuitively speaking U can be obtained by taking an arbitrary ordering on the subspace that Q identifies with 1. To see this, denote the ordering induced by the addition on $\mathbb{B}[\boldsymbol{x}^{\pm 1}]/Q$ by $\leq_Q$ and fix an arbitrary term ordering $\preceq_0$. Now we define a new term ordering $\preceq$ as

$$m_1 \preceq m_2 \iff m_1 <_Q m_2 \text{ or } [(m_1, m_2) \in Q \text{ and } m_1 \preceq_0 m_2].$$

To verify that $\preceq$ is indeed a term ordering consider m_1, m_2 such that $m_1 \preceq m_2$ and an arbitrary monomial $s \neq 0$. We have that either $m_1 <_Q m_2$, but then by the cancellativity of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]/Q$ it follows that $sm_1 <_Q sm_2$, or $(m_1, m_2) \in Q$ and $m_1 \preceq_0 m_2$ and then since Q is a congruence and $\preceq_0$ is a term ordering we have that $(sm_1, sm_2) \in Q$ and $sm_1 \preceq_0 sm_2$. Now from the definition of $\preceq$ we see that $m_1 \preceq m_2 \Rightarrow m_1 \leq_Q m_2$, so for the defining matrix U of $\preceq$ we have $P(U) \subseteq Q$. □

A *lattice polytope* in $\mathbb{R}^k$ is just a polytope whose vertices are all in $\mathbb{Z}^k$. The *Newton polytope* of a polynomial $f = \sum_i \boldsymbol{x}^{\boldsymbol{n}_i}$ of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ or $\mathbb{B}[\boldsymbol{x}]$ is the convex hull of the lattice points $\boldsymbol{n}_i \in \mathbb{Z}^k$. It will be denoted by $newt(f)$. By convention $newt(0)$ is the empty set. Now we proceed to describe the prime congruences and radical of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$. We remind that by convention we also write the maximal congruence of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ as $P(U)$ where U is a matrix with "zero rows".

Theorem 5.1.7. *For the k-variable Laurent polynomial semialgebra $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ we have that:*

(i) The set of prime congruences of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ is $\{P(U) \mid U \text{ is an admissible matrix with } k \text{ columns}\}$. The prime congruence $P(U)$ is minimal if and only if $Ker(U) \cap \mathbb{Z}^k = \{\mathbf{0}\}$.

(ii) $dim(\mathbb{B}[\boldsymbol{x}^{\pm 1}]) = k$.

(iii) The pair (f, g) lies in the radical of the trivial congruence of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ if and only if $newt(f) = newt(g)$.

(iv) The $\mathbb{B}$-algebra $\mathbb{B}[\boldsymbol{x}^{\pm 1}]/Rad(\Delta)$ is isomorphic to the $\mathbb{B}$-algebra with elements the lattice polytopes and addition being defined as the convex hull of the union, and multiplication as the Minkowski sum.

(v) Every radical congruence is QC.

Proof. For (i) consider that by Lemma 5.1.6 every prime contains a prime $P(U)$ with $Ker(U) \cap \mathbb{Z}^k = \{\mathbf{0}\}$ and by Proposition 5.1.5 every prime lying over some $P(U)$ is $P(U(i))$ for some $0 \leq i \leq r(U)$. (ii) follows from Proposition 5.1.5 and the fact that there are term orderings whose defining series is of length k (for example the usual lexicographic order). For (iii) first note that since every prime is contained in a minimal prime the radical of the trivial congruence is the intersection of the minimal primes. By (i) a minimal prime $P(U)$ corresponds to a term ordering, and for a monomial m and a polynomial f we have $(f, m) \in P(U)$ if and only if m is the leading term of f in the corresponding term ordering. Hence it is enough to show that the set of vertices of $newt(f)$ are precisely the exponents of the monomials of f that are leading terms with respect to some term ordering. On one hand by Proposition 5.1.3 the leading term is determined by maximizing a set of linear functionals on $newt(f)$, so its exponent indeed has to be one of the vertices. On the other hand for any vertex v of $newt(f)$ one can pick a hyperplane that separates it from the rest of the vertices. Choosing the normal vector $\boldsymbol{u}$ of such a hyperplane to point towards the side of v, for any admissible matrix U with $Ker(U) \cap \mathbb{Z}^k = \{\mathbf{0}\}$ having $\boldsymbol{u}$ as a first row we have that the leading term of f in the term ordering defined by U is the monomial with exponent v. Now since the set of vertices determine the polytope $newt(f)$ we have that (f, g) lies in every prime if and only if $newt(f) = newt(g)$. For (iv) one easily checks that $newt(f + g)$ is the convex hull of $newt(f) \cup newt(g)$ and $newt(fg)$ is the Minkowski sum of $newt(f)$ and $newt(g)$. For (v) assume that for a radical congruence I, $(g,0)(f_1,f_2) \in I$ then $(g,0)(f_1,f_2)$ is in every prime containing I, but since all primes have trivial kernels (f_1,f_2) has to be in every prime containing I and then $(f_1,f_2) \in I$. □

In the one variable case there are only finitely many primes are the radical is easily computable,

Example 5.1.8. Let P be a prime of the one variable Laurent polynomial semiring $\mathbb{B}(x)$. Then by Proposition 5.1.2 the quotient $\mathbb{B}(x)/P$ is totally ordered and hence we have one of the three options $1 = x$ or $x > 1$ or $1 > x$.

- If $1 = x$ then P is the congruence that identifies every non-zero element with 1. Thus P is a maximal congruence and $\mathbb{B}(x)/P = \mathbb{B}$.
- If $x > 1$ then $x^i > x^j$ whenever $i > j$, so P identifies every polynomial with it is highest degree term, and $\mathbb{B}(x)/P = \mathbb{Z}_{max}$.
- If $1 > x$ then every polynomial is identified with its lowest degree term and $\mathbb{B}(x)/P = \mathbb{Z}_{min}$.

We obtained that $\mathbb{B}(x)$ has precisely 3 prime congruences. It is easy to see that $Rad(\Delta)$ is then the congruence that identifies two polynomials if their highest and lowest degree terms agree. As expected by Theorem 5.1.7 $Rad(\Delta)$ is QC, however it is clearly not prime.

However, in the case of two or more variables there are infinitely many primes, hence by Proposition 3.3.1 we have the following corollary:

Corollary 5.1.9. *If $k > 1$ there are infinitely many minimal prime congruences in $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ and if $k = 1$ there are exactly two. In particular for $k > 1$ $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ does not satisfy the ACC for radical congruences (or equivalently for QC congruences).*

Now we turn to $\mathbb{B}[\boldsymbol{x}]$. Recall from (iii) of Proposition 5.1.2 that the primes of $\mathbb{B}[\boldsymbol{x}]$ with trivial kernel are restrictions of the primes of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$. Here we also have over any prime $P[U]$ the strictly increasing chain

$$P[U] = P[U(r(U))] \subset P[U(r(U)-1)] \subset \cdots \subset P[U(0)].$$

It follows that $dim(P[U]) \geq dim(P(U)) = r(U)$, the next proposition shows that the dimensions are in fact equal.

Proposition 5.1.10. *For any admissible matrix U we have that $dim(\mathbb{B}[\boldsymbol{x}]/P[U]) = r(U)$.*

Proof. We will prove by induction on $r(U)$. The $r(U) = 0$ case is clear, since by our earlier conventions for the matrix with "zero rows" we have $\mathbb{B}[\boldsymbol{x}]/P[U] = \mathbb{B}$ and $dim(\mathbb{B}) = 0$. Let U now be an arbitrary admissible matrix and Q a prime congruence that is minimal amongst those that strictly contain $P[U]$, to complete the proof we need to show that $dim(Q) \leq r(U)-1$. If $Ker(Q) = \{0\}$ then by (iii) of Proposition 5.1.2 and Proposition 5.1.5 we have that $Ker(Q) = P[U(r(U)-1)]$ and then by the induction hypothesis we have $dim(Q) = r(U)-1$. If $Ker(Q) \neq \{0\}$ then by Proposition 5.1.1, $Ker(Q)$ is generated by a subset of the variables, say $x_1, \dots, x_j$. Also by the minimality of Q we have that $Q = \langle P(U) \cup \{(x_i, 0) | 1 \leq i \leq j\}\rangle$. It follows that for some prime $P[U_Q]$ of $\mathbb{B}[x_{j+1}, \dots, x_k]$ the quotient $\mathbb{B}[\boldsymbol{x}]/Q$ is isomorphic to $\mathbb{B}[x_{j+1}, \dots, x_k]/P[U_Q]$. The matrix U_Q can be obtained from U by removing the first j columns, then removing any possible redundant rows. Now since $(1,0) \notin Q$ by (iii) of Proposition 3.1.4 we have that for any monomial m containing any of the variables $x_1, \dots, x_j$, $m < 1$ in the ordering defined by U. This implies that the for some $1 \leq i \leq r(U)$ the first i rows of U have to be such that all non-zero entries are in the first j columns, and the first non-zero entry in those columns is negative. Consequently when the first j columns are removed from U, then the first i rows will have all 0-s as the remaining entries, so they are removed when we obtain U_Q. In particular we have that $dim(Q) = r(U_Q) < r(U)$ completing the proof. □

Now we have the following theorem about the primes and radical of $\mathbb{B}[\boldsymbol{x}]$:

Theorem 5.1.11. *For the k-variable polynomial semiring $\mathbb{B}[\boldsymbol{x}]$ we have that,*

(i) For every prime congruence P of $\mathbb{B}[\boldsymbol{x}]$ there is a (possibly empty) subset H of the variables $\boldsymbol{x}$ and a prime $P[U]$ of the polynomial semiring $\mathbb{B}[\boldsymbol{x'}]$ with variables $\boldsymbol{x'} = \boldsymbol{x} \setminus H$, such that P is generated by the pairs $\{(x_i, 0) | \; x_i \in H\}$ and the image of $P[U]$ under the embedding $\mathbb{B}[\boldsymbol{x'}] \hookrightarrow \mathbb{B}[\boldsymbol{x}]$.

(ii) The minimal prime congruences of $\mathbb{B}[\boldsymbol{x}]$ have $\{0\}$ as their kernel and are all of the form $P[U]$, where U is an admissible matrix with $Ker(U) \cap \mathbb{Z}^k = \{\mathbf{0}\}$.

(iii) $dim(\mathbb{B}[\boldsymbol{x}]) = k$.

(iv) The pair (f, g) lies in the radical of the trivial congruence of $\mathbb{B}[\boldsymbol{x}]$ if and only if $newt(f) = newt(g)$.

(v) The $\mathbb{B}$-algebra $\mathbb{B}[\boldsymbol{x}]/Rad(\Delta)$ is isomorphic to the $\mathbb{B}$-algebra with elements the lattice polytopes lying in the non negative quadrant $\mathbb{R}^k_{+,0}$, and addition being defined as the convex hull of the union, and multiplication as the Minkowski sum.

(vi) The congruence $Rad(\Delta)$ is QC.

Proof. (i) follows from Proposition 5.1.1, Theorem 5.1.7 and (iii) of Proposition 5.1.2. For (ii) let Q be a minimal prime congruence with $Ker(Q) \neq 0$. We can assume that $Ker(Q)$ is generated by the variables $x_1, \ldots, x_j$ for some j. By the minimality of Q, $\mathbb{B}[\boldsymbol{x}]/Q$ is isomorphic to $P[U']$ where U' is the defining matrix of a term ordering on the variables $x_{j+1}, \ldots, x_k$. Let U be the defining matrix of the term ordering that first orders the variables $x_1, \ldots, x_j$ reverse lexicographically, then the rest of the variables by U' (so the first j rows of U are negatives of the first j rows of the identity matrix). Now for the prime congruence $P[U]$ we have $Ker(P[U]) = \{0\}$ and $P[U] \subseteq Q$. (iii) follows from (ii) and Proposition 5.1.10. (iv) and (v) follow by the same argument as in the proof of Theorem 5.1.7. Finally (vi) also follows the same way as in Theorem 5.1.7 after considering that the radical is the intersection of the minimal primes and minimal primes of $\mathbb{B}[\boldsymbol{x}]$ have trivial kernels. □

We finish this section by providing an explicit description of the defining matrices of prime congruences above which lie primes with non-trivial kernel.

Lemma 5.1.12. *Let P be a prime of $\mathbb{B}[x_1, \ldots, x_n]$ with trivial kernel and defining matrix U and let the first row of this matrix be given by the vector $(a_1,\ a_2, \ldots, a_n)$. Let Q be a prime lying above P such that $Ker(Q)$ is generated by only one of the variables, say x_1. Then $a_1 < 0$ and $a_i = 0$, for all $2 \leq i \leq n$.*

Proof. Assume for contradiction that $a_1 > 0$, this means that $x_1 > 1$ but $(x_1, 0) \in P$ which in turn implies that $(1, 0) \in P$ which is a contradiction since P is a proper congruence. If $a_1 = 0$ and $a_2 > 0$ then $x_1x_2 > 1$ thus $(1, 0) \in Q$, again a contradiction. However if $a_2 < 0$, then $x_1 > x_2$ and this implies that $(x_2, 0) \in Q$ contradiction, since $x_2 \notin Ker(Q)$. Hence $a_1 < 0$. Looking at the rest of the a_i's, if $a_2 > 0$ then for some $l, k \in \mathbb{N}$ and k big enough, ${x_1}^l {x_2}^k > 1$, thus $(1, 0) \in Q$. Alternatively if $a_2 < 0$, take $l \in \mathbb{N}$ big enough, then ${x_2}^l < x_1$. Then by primeness of Q and $x_1 \in Ker(Q)$ we get that $x_2 \in Ker(Q)$, contradiction. □

Proposition 5.1.13. *Let P be a prime with trivial kernel of $\mathbb{B}[\boldsymbol{x}]$ with defining matrix U. Let Q be a prime lying above P such that $Ker(Q)$ be generated by a subset of the variables, say $\{x_1, \ldots, x_k\}$. Then $U = \begin{bmatrix} A & \mathbf{0} \\ B & C \end{bmatrix}$, where A is a $l \times k$ admissible matrix, $l \leq k$ and first entry of every column is negative. Furthermore C is also admissible and $Q = P[C]$.*

Proof. The statement follows directly from Lemma 5.1.12. Admissibility is obvious since $P[A] = P[U(i)]$, where i is the number of rows of B. □

Remark 5.1.14. *In the set up of Proposition 5.1.13 the columns corresponding to the variables in the kernel of Q are a linear combination of the first column and the columns of* $\begin{bmatrix} \mathbf{0} \\ C \end{bmatrix}$.

5.2 The prime congruences of $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ and $\mathbb{Z}_{max}[\boldsymbol{x}]$

The description of the primes and the radical of $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ and $\mathbb{Z}_{max}[\boldsymbol{x}]$ can be easily derived from that of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ and $\mathbb{B}[\boldsymbol{x}]$. The key observation is that $\mathbb{Z}_{max} \cong \mathbb{B}(t)/\langle(1+t,t)\rangle$ and consequently $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}] = \mathbb{B}(t,\boldsymbol{x})/\langle(1+t,t)\rangle$ where $\mathbb{B}(t,\boldsymbol{x})$ is just the semiring of Laurent polynomials over $\mathbb{B}$ with $k+1$ variables $(t, x_1, \dots, x_k)$. Hence prime congruences of $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ can be identified with the prime congruences of $\mathbb{B}(t,\boldsymbol{x})$ containing $(t, 1+t)$. By Theorem 5.1.7 these are of the form $P(U)$ where U is an admissible matrix with $k+1$ columns, such that the either its first column has all 0 entries or the first non-zero entry of the first column is positive. We will call such a matrix *z-admissible*, and we will denote the congruence defined by it in $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ by $P(U)_{\mathbb{Z}}$ and its restriction to $\mathbb{Z}_{max}[\boldsymbol{x}]$ by $P[U]_{\mathbb{Z}}$.

By the Newton polytope, *newt*(f), of a polynomial $f = \sum_i t^{c_i} \boldsymbol{x}^{\boldsymbol{n}_i}$ in $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ or $\mathbb{Z}_{max}[\boldsymbol{x}]$, we mean the convex hull of the points $[c_i, \boldsymbol{n}^i] \in \mathbb{Z}^{k+1}$. We define the *hat* of *newt*(f) to be the set

$$\overline{newt(f)} = \{(y_0, \dots, y_k) \in newt(f) \mid \forall z > y_0 : \ (z, y_1, \dots, y_k) \notin newt(f)\}.$$

We have the following theorem:

Theorem 5.2.1. *For the k-variable polynomial semiring $\mathbb{Z}_{max}[\boldsymbol{x}]$ and the k-variable Laurent polynomial semiring $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ we have that:*

(i) The minimal primes of $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ (resp. $\mathbb{Z}_{max}[\boldsymbol{x}]$) are of the form $P(U)_{\mathbb{Z}}$ (resp. $P[U]_{\mathbb{Z}}$) for a z-admissible matrix U with $k+1$ columns satisfying $Ker(U) \cap \mathbb{Z}^{k+1} = \{\mathbf{0}\}$.

(ii) $dim(\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]) = dim(\mathbb{Z}_{max}[\boldsymbol{x}]) = k+1$

(iii) For any $f, g \in \mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ (resp. $f, g \in \mathbb{Z}_{max}[\boldsymbol{x}]$) the pair (f,g) lies in the radical of the trivial congruence of $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ (resp. $\mathbb{Z}_{max}[\boldsymbol{x}]$) if and only if $\overline{newt(f)} = \overline{newt(g)}$.

(iv) Every congruence of $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ is QC. $Rad(\Delta)$ in $\mathbb{Z}_{max}[\boldsymbol{x}]$ is QC.

Proof. (i) and (ii) follows from the discussion preceding the theorem. For (iii) by the same argument as in the proof of Theorem 5.1.7 we need to show that the vertices of $\overline{newt(f)}$ are precisely the exponents of the monomials of f that are maximal with respect to the ordering in the quotient of some minimal prime. By (i) we have that in both cases minimal primes correspond to term orderings of the variables $(t, \boldsymbol{x})$ such that $1 < t$ and it is clear that the leading monomial of f with respect to such a term ordering has to be one of the vertices lying on $\overline{newt(f)}$. For the other direction for a vertex v on $\overline{newt(f)}$ let $\boldsymbol{u}$ be a linear combination with positive coefficients of the outwards pointing normal vectors of the k-dimensional faces of $\overline{newt(f)}$ containing v, such that the first coordinate of $\boldsymbol{u}$ is positive. Such a $\boldsymbol{u}$ can be chosen since the outwards pointing normal vector of any k-dimensional face of $\overline{newt(f)}$ have positive first coordinate, so if we set the coefficients corresponding to those faces large enough $\boldsymbol{u}$ will also have a positive first coordinate. Moreover v is the unique vertex that maximizes the scalar product taken with $\boldsymbol{u}$ on $\overline{newt(f)}$. Hence we can choose a z-admissible matrix U with $\boldsymbol{u}$ as its first row and $Ker(U) \cap \mathbb{Z}^{k+1} = \{\mathbf{0}\}$ and in the term ordering defined by U the leading term of f will be the monomial with exponent v. Finally (iv) follows the same way as in Theorems 5.1.7 and 5.1.11. □

5.3 The prime congruences of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ and $\mathbb{T}[\boldsymbol{x}]$

In this section we describe the primes and the radical of the semirings of polynomials and Laurent polynomials with coefficients in $\mathbb{T}$.

A matrix U whose first column has either all zero entries or its first non-zero entry is positive can define a prime congruence $P(U)_{\mathbb{T}}$ of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$, which, as in the previous cases is generated by pairs $(t^{c_1}\boldsymbol{x}^{\boldsymbol{n}_1} + t^{c_2}\boldsymbol{x}^{\boldsymbol{n}_2}, t^{c_2}\boldsymbol{x}^{\boldsymbol{n}_2})$ such that $U((c_2, \boldsymbol{n}_2) - (c_1, \boldsymbol{n}_2))$ is either the $\mathbf{0}$ vector or its first non-zero coordinate is positive. Clearly if U is z-admissible and we consider $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$ as a subsemiring of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$, we have $P(U)_{\mathbb{T}}|_{\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]} = P(U)_{\mathbb{Z}}$. However $P(U)_{\mathbb{T}}$ might not be the only congruence that restricts to $P(U)_{\mathbb{Z}}$ as shown by the following example:

Example 5.3.1. Let $r \in \mathbb{R}$ be an irrational number and let U be the matrix that consists of the single line $[1\ r]$. Since $Ker(U) \cap \mathbb{Z}^2 = \{\mathbf{0}\}$, U defines a total ordering on $\mathbb{Z}^2$ and hence $P(U)$ is a minimal prime of $\mathbb{B}(x_1, x_2)$ and $P(U)_{\mathbb{Z}}$ is a minimal prime of $\mathbb{Z}_{max}(x_1)$. Consequently any subsequent rows to U would be redundant. However $Ker(U) \cap \mathbb{R} \oplus \mathbb{Z} \neq \{0\}$, so U does not define a total ordering on the monomials of $\mathbb{T}(x_1)$, and one can add a subsequent row to U which will give the ordering on the elements in $Ker(U) \cap (\mathbb{R} \oplus \mathbb{Z})$. For example denoting by U_+ the matrix which is obtained from U by adding the row $[0\ 1]$ and U_- the matrix which is obtained by adding the row $[0\ -1]$, we have that $P(U_+)_{\mathbb{T}}$ and $P(U_+)_{\mathbb{T}}$ are distinct minimal primes of $\mathbb{T}(x_1)$ both strictly containing $P(U)_{\mathbb{T}}$, and $P(U_+)_{\mathbb{T}}|_{\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]} = P(U_-)_{\mathbb{T}}|_{\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]} = P(U)_{\mathbb{T}}|_{\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]} = P(U)_{\mathbb{Z}}$.

Motivated by this example we define an $l \times (k+1)$ matrix U to be *t-admissible* if its rows are non-redundant with respect to the ordering defined on $\mathbb{R} \oplus \mathbb{Z}^k$, i.e. for every $1 \leq i \leq l$ there is a $\boldsymbol{v} \in \mathbb{R} \oplus \mathbb{Z}^k$ such that the i-th is the first non-zero entry of $U\boldsymbol{v}$ moreover we require that in the first column of U either all of the entries are 0 or its first non-zero entry is positive. Clearly z-admissible matrices are also t-admissible, but some t-admissible matrices, like U_+ and U_- from the above example, might not be z-admissible. Then the prime congruence $P(U)_{\mathbb{T}}$ is defined for all t-admissible matrices U, and $P(U)_{\mathbb{T}}|_{\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]} = P(U')_{\mathbb{Z}}$ where U' is the matrix we obtain from U after removing rows that become redundant when U defines an ordering of the monomials with coefficients in $\mathbb{Z}_{max}$. The restriction of $P(U)_{\mathbb{T}}$ to $\mathbb{T}[\boldsymbol{x}]$ will be denoted by $P[U]_{\mathbb{T}}$. As previously, we aim to show that all primes of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ are of the form $P(U)$ for a t-admissible U. For this we will need the following variation on the result from [Rob85] which we recalled in Proposition 5.1.3.

Lemma 5.3.2. *For any group ordering $\preceq$ on the multiplicative group of the monomials of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ satisfying that for every $c_1, c_2 \in \mathbb{R}$ and $\boldsymbol{n} \in \mathbb{Z}^k$ we have that $t^{c_1}x^{\boldsymbol{n}_1} \preceq t^{c_2}x^{\boldsymbol{n}_2}$ if and only if $c_1 \leq c_2$ by the usual ordering on $\mathbb{R}$, there exits a t-admissible matrix U such that $t^{c_1}x^{\boldsymbol{n}_1} \prec t^{c_2}x^{\boldsymbol{n}_2}$ if and only if the first non-zero coordinate of $U((c_2, \boldsymbol{n}_2) - (c_1, \boldsymbol{n}_1))$ is positive.*

Proof. First note that the multiplicative group of the monomials of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ is isomorphic to the additive group $(\mathbb{R} \oplus \mathbb{Z}^k, +)$. It follows from Lemma 1 of [Rob85] (and can also be easily checked) that every group ordering of $(\mathbb{R} \oplus \mathbb{Z}^k, +)$ uniquely extends to a group ordering of $G = (\mathbb{R} \oplus \mathbb{Q}^k, +)$. By a slight abuse of notation let us denote the ordering induced on G by $\preceq$ as well. Let G_+ denote the set $\{\boldsymbol{v} \in G | \boldsymbol{v} \succ \boldsymbol{0}\}$ and G_- denote the set $\{\boldsymbol{v} \in G | \boldsymbol{v} \prec \boldsymbol{0}\}$. Now following the original argument from [Rob85] we define I_G to be the set of points $p \in \mathbb{R}^{k+1}$ such that each open (Euclidean) neighbourhood of p contains elements from both G_+ and G_-. It is easy to verify that I_G is a linear subspace. Let V_+ (resp. V_-) denote the open set in $\mathbb{R}^k$ that consists of points with an open neighbourhood that does not intersect G_- (resp. G_+). Now we have that $\mathbb{R}^{k+1} \setminus I_G = V_- \cup V_+$, so the complement of I_G is the union of disjoint open sets and hence disconnected, it follows that $dim(I_G) \geq k$. On the other hand V_+ and V_- each contain at least an open quadrant, so $dim(I_G) = k$. Let us note that this is where the argument would fail if one wanted to extend it to an arbitrary group ordering on $\mathbb{R} \oplus \mathbb{Z}^k$, but in our case, due to the the elements of $\mathbb{R} \oplus \{\boldsymbol{0}\}$ being ordered in the usual way, for the vector $\boldsymbol{e}_0 = (1, 0, \ldots, 0)$ and a $\mathbb{Z}$-basis $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$ of $\mathbb{Z}^k$ satisfying $\boldsymbol{e}_i \succ \boldsymbol{0}$, we have that the the positive $\mathbb{R}$-linear combinations of $\boldsymbol{e}_0, \ldots, \boldsymbol{e}_k$ are indeed in V_+ and the negatives of these are in V_-. Now for the normal vector $\boldsymbol{u}$ of I_G pointing towards V_+ and any $\boldsymbol{v}_1, \boldsymbol{v}_2 \in G$ we have that $\boldsymbol{u} \cdot (\boldsymbol{v}_2 - \boldsymbol{v}_1) > 0 \Rightarrow \boldsymbol{v}_1 \prec \boldsymbol{v}_2$, where $\cdot$ denotes the usual scalar product on $\mathbb{R}^{k+1}$, so $\boldsymbol{u}$ can be chosen as the first row of U. Moreover the subgroup $G_0 = \{\boldsymbol{v} \in G | \boldsymbol{u} \cdot \boldsymbol{v} = 0\}$ is isomorphic to $\mathbb{Z}^k$ when the first coordinate of $\boldsymbol{u}$ is non-zero, and it is isomorphic to $\mathbb{R} \oplus \mathbb{Z}^l$ for some $l < k$ if the first coordinate of $\boldsymbol{u}$ is zero. Hence either by Proposition 5.1.3 or by induction we have that the ordering on G_0 is given by a matrix with at most k rows, and by adding to that matrix $\boldsymbol{u}$ as a first row we obtain the U in the lemma. □

In the following proposition we will list the analogues of Propositions 5.1.2/(iii), 5.1.1, 5.1.5, 5.1.10 and Lemma 5.1.6 for $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ and $\mathbb{T}[\boldsymbol{x}]$. We will omit the proofs since they are essentially the same as in the previous section. Recall that $U(i)$ denotes the matrix that consists of the first i rows of U.

Proposition 5.3.3. *(i) Primes of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ always have $\{0\}$ as their kernel, and the kernel of a prime in $\mathbb{T}[\boldsymbol{x}]$ is generated by a subset of the variables $\boldsymbol{x}$.*

(ii) If Q is a prime congruence of $\mathbb{T}[\boldsymbol{x}]$ with $Ker(Q) = \{0\}$, then $Q = P|_{\mathbb{T}[\boldsymbol{x}]} = P$ for some prime congruence P of of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$.

(iii) Every congruence of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ containing some $P(U)_{\mathbb{T}}$ for an $l \times (k+1)$ t-admissible matrix U is of the form $P(U(i))_{\mathbb{T}})$ for some $0 \leq i \leq l$.

(iv) For an $l \times (k+1)$ t-admissible matrix U, we have $dim(\mathbb{T}[\boldsymbol{x}^{\pm 1}]/P(U)_{\mathbb{T}}) = dim(\mathbb{T}[\boldsymbol{x}]/P[U]_{\mathbb{T}}) = r(U) = l$.

(v) Every prime of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$, contains a prime $P(U)_{\mathbb{T}}$ for a t-admissible matrix U with $Ker(U) \cap \mathbb{R} \oplus \mathbb{Z}^k = \{\boldsymbol{0}\}$.

Similarly to the previous cases the Newton polytope, *newt*(f), of a polynomial $f = \sum_i t^{c_i} \boldsymbol{x}^{\boldsymbol{n}_i}$ in $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ or $\mathbb{T}[\boldsymbol{x}]$, we mean the convex hull of the points $[c_i, \boldsymbol{n}_i] \in \mathbb{R} \oplus \mathbb{Z}^k$. The hat of the Newton polytope is defined the same way as in the case of $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$.

Now we are ready to describe the primes and the radicals of $\mathbb{T}[\boldsymbol{x}]$ and $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$, which is analogous to the previous cases studied, except that this time we need to consider t-admissible matrices for defining prime congruences.

Theorem 5.3.4. *For the k-variable polynomial semiring $\mathbb{T}[\boldsymbol{x}]$ and the k-variable Laurent polynomial semiring $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ we have that:,*

(i) Every prime congruence of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ is of the form $P(U)_{\mathbb{T}}$ for a t-admissible matrix U. For every prime congruence P of $\mathbb{T}[\boldsymbol{x}]$ there is a (possibly empty) subset H of the variables $\boldsymbol{x}$ and a prime

$P[U]$ of the polynomial semiring $\mathbb{T}[\boldsymbol{x}']$ with variables $\boldsymbol{x}' = \boldsymbol{x} \setminus H$, such that P is generated by the pairs $\{(x_i, 0) |\, x_i \in H\}$ and the image of $P[U]$ under the embedding $\mathbb{T}[\boldsymbol{x}'] \hookrightarrow \mathbb{T}[\boldsymbol{x}]$.

(ii) The minimal prime congruences of $\mathbb{T}[\boldsymbol{x}]$ have $\{0\}$ as their kernel. Every minimal prime of $\mathbb{T}[\boldsymbol{x}]$ (resp. $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$) is of the form $P[U]_{\mathbb{T}}$ (resp. $P(U)_{\mathbb{T}}$), where U is a t-admissible matrix with $Ker(U) \cap \mathbb{R} \oplus \mathbb{Z}^k = \{\boldsymbol{0}\}$.

(iii) $dim(\mathbb{T}[\boldsymbol{x}^{\pm 1}]) = dim(\mathbb{T}[\boldsymbol{x}]) = k + 1$.

(iv) For any $f, g \in \mathbb{T}[\boldsymbol{x}^{\pm 1}]$ (resp. $f, g \in \mathbb{T}[\boldsymbol{x}]$) the pair (f, g) lies in the radical of the trivial congruence of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ (resp. $\mathbb{T}[\boldsymbol{x}]$) if and only if $\overline{newt(f)} = \overline{newt(g)}$.

(v) Every congruence of $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ is QC. Rad(Δ) in $\mathbb{T}[\boldsymbol{x}]$ is QC.

Proof. (ii) follows from Lemma 5.3.2, and the rest of the theorem follows from Proposition 5.3.3 by the same arguments as in Theorems 5.1.7, 5.1.11 and 5.2.1. □

5.4 Prime congruences of $\mathbb{R}^n_{lex} \cup \{-\infty\}$

To end this chapter we introduce an idempotent semifield which is not a subsemifield of $\mathbb{T}$. This is the semifield $\mathbb{R}^n_{lex} \cup \{-\infty\}$ which we denote by $\mathbb{T}_n$. Its underlying set is $\mathbb{R}^n \cup \{-\infty\}$. The two operations are lexicographical ordering playing the role of addition and multiplication - the usual vector addition, which we will denote by $\odot$. Note that this is a totally ordered semifield thus a domain. We would like to remark that $\mathbb{T}_n$ is not $\mathbb{T}^n$, which contains non-invertible elements. However, when $n = 1$ then $\mathbb{T}_n$ is just $\mathbb{T}$.

Proposition 5.4.1. *The prime congruences of $\mathbb{T}_n$ are kernels of morphisms $\mathbb{T}_n \to \mathbb{T}_{n-k}$, for some $k \in \mathbb{N}$.*

Proof. Let P be a prime $\mathbb{T}_n$ and $(\boldsymbol{a}, \boldsymbol{b}) \in P$, where $\boldsymbol{a} = (a_1, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, \ldots, b_n)$.

If $a_1 \neq b_1$, then without loss of generality $a_1 < b_1$ thus $\boldsymbol{a} < \boldsymbol{b}$, by which we mean $\boldsymbol{a} <_{lex} \boldsymbol{b}$. Then there exists a $\boldsymbol{v} \in \mathbb{T}_n$ with $a_1 < v_1 < b_1$ so let $\boldsymbol{v} = \boldsymbol{a} \odot \boldsymbol{\epsilon} = (a_1 + \epsilon, \ldots, a_n + \epsilon)$, for some $\epsilon > 0$. Then we get $\boldsymbol{a} < \boldsymbol{a} \odot \boldsymbol{\epsilon} < \boldsymbol{b} < \boldsymbol{b} \odot \boldsymbol{\epsilon}$. Since $(\boldsymbol{a}, \boldsymbol{b}) \in P$ then $(\boldsymbol{a}, \boldsymbol{a} \odot \boldsymbol{\epsilon}) \in P$ and hence $(\boldsymbol{a}, \boldsymbol{b} \odot \boldsymbol{\epsilon})$. This way we obtain $(\boldsymbol{a}, \boldsymbol{u}) \in P$, for every $\boldsymbol{u} \in \mathbb{R}^n$. Thus all vectors in $\mathbb{T}_n \setminus \{-\infty\}$ are congruent to each other. In this case we obtain a maximal congruence with quotient $\mathbb{B}$.

If $a_i = b_i$, for some $1 \leq i \leq k$, then assume again $\boldsymbol{a} < \boldsymbol{b}$ and that there exists $\boldsymbol{v}$, with $\boldsymbol{a} < \boldsymbol{v} < \boldsymbol{b}$ and $a_i = v_i = b_i$, for $1 \leq i \leq k$. Then if $\forall (\boldsymbol{a}, \boldsymbol{b}) \in P$, the first i coordinates are the same, then P is a prime with $\mathbb{T}_n / P = \mathbb{T}_{n-k}$. □

Corollary 5.4.2. *The dimension of* $\mathbb{T}_n$ *is* n*.*

Proof. Follows directly from Proposition 5.4.1. □

6

Tropical Nullstellensatz

We show that for any finitely generated congruence C in a polynomial or Laurent polynomial semiring over $\mathbb{B}$, $\mathbb{Z}_{max}$ or $\mathbb{T}$, $Rad(C)$ is the intersection of the primes that contain C and have a quotient with dimension 1. This result is an analogue to the classical statement that in a polynomial ring over a field every radical ideal is the intersection of maximal ideals.

In this section we regard the elements of the k-variable semiring $\mathbb{T}[\boldsymbol{x}]$ as functions on the set $\mathbb{T}^k$. For a congruence C denote by $\mathbb{V}(C)$ the subset of $\mathbb{T}^k$ where every congruent pair from C gives the same value. For a subset H of $\mathbb{T}^k$ we denote by $\mathbb{E}(H)$ the congruence that identifies polynomials that agree on every point of H. In this terminology the aim of a "tropical Nullstellensatz" is to describe the set $\mathbb{E}(\mathbb{V}(C))$ for a finitely generated congruence C. We show that this set is obtained as the intersection of the geometric congruences (congruences with quotient $\mathbb{T}$), hence is a congruence itself and is described by generalized powers.

6.1 The Tropical Nullstellensatz Problem

The problem of finding an analogue of the Nullstellensatz for the tropical semifield $\mathbb{T}$ was raised by A. Bertram and R. Easton in [BE13]. For a congruence C of the k-variable polynomial semiring $\mathbb{T}[\boldsymbol{x}]$ we consider the following set,

$$\mathbb{V}(C) = \{v \in \mathbb{T}^k \mid f(v) = g(v),\, \forall (f, g) \in C\}.$$

For a subset $H \subseteq \mathbb{T}^k$ we define the congruence

$$\mathbb{E}(H) = \{(f,g) \in \mathbb{T}[\boldsymbol{x}] \times \mathbb{T}[\boldsymbol{x}] \mid f(v) = g(v) \, \forall v \in H\}.$$

The aim of a "Tropical Nullstellensatz" is to describe the set $\mathbb{E}(\mathbb{V}(C))$ with some suitable power formulas, when C is finitely generated. In [BE13] for a congruence C the set C_+ is defined to consist of all pairs (f,g) for which there exist $1 \neq \epsilon \in \mathbb{T}$, $h \in \mathbb{T}[\boldsymbol{x}]$ and a non-negative integer i, such that:

$$(1,\epsilon)((f,g)^{*i} + (h,0))(f,g) \in C.$$

Moreover it is shown that C_+ consists of certain limits of pairs of elements that lie in $\mathbb{E}(\mathbb{V}(C))$. In Theorem 3 of [BE13], and in the discussion preceding it, it was established that $C \subseteq C_+ \subseteq \mathbb{E}(\mathbb{V}(C))$ and $\mathbb{V}(C) = \mathbb{V}(C_+)$, moreover that if C is finitely generated then the set $\mathbb{V}(C)$ is empty if and only if $C_+ = \mathbb{T}[\boldsymbol{x}] \times \mathbb{T}[\boldsymbol{x}]$.

However two questions were left open, namely whether one has $C_+ = \mathbb{E}(\mathbb{V}(C))$ for all finitely generated C and if the set C_+ is a congruence in general. The aim of Section 6.3 is to show that the answer to both these questions is positive.

Example 6.1.1. In the 2-variable semiring $\mathbb{T}[x,y]$ consider the congruence $C = \langle (x^2, y^2) \rangle$. Since for $a, b \in \mathbb{T}$ we have

$$a^2 = b^2 \Leftrightarrow a = b$$

one can easily see that

$$\mathbb{V}(C) = \{(a,a) \mid a \in \mathbb{T}\}$$

It follows that $(x,y) \in \mathbb{E}(\mathbb{V}(C))$. Moreover it is easy to see that $\mathbb{E}(\mathbb{V}(C)) = \langle (x,y) \rangle$. Recall that we saw earlier in Example 3.2.4 that $(x,y) \in Rad(C)$. However $(x,y)^n$ is not in C for any n. In fact this happens since some generalized power of (x,y) lies in the congruence C and $Rad(C) \subseteq \mathbb{E}(\mathbb{V}(C))$.

6.2 Maximal and Geometric congruences

We give a characterization of a class of congruences which will be central to the solution of the Nullstellensatz problem. In commutative algebra maximal ideals of a polynomial ring $k[\boldsymbol{x}]$ over a field k are the kernels of evaluation morphisms and the quotient by a maximal ideal is the underlying field k. However maximal congruences of idempotent semifields are not the kernels of evaluation morphisms and for every idempotent semifield A, the maximal congruences of $A[\boldsymbol{x}]$ have quotient $\mathbb{B}$. Moreover there are very few maximal congruences as shown in the following proposition.

Proposition 6.2.1. *In the polynomial semiring $A[x_1, \dots, x_n]$, where A is a semifield there are 2^n maximal congruences which are in one to one correspondence with saturated prime ideals.*

Proof. Consider the surjective semiring morphism $\phi : A[x_1, \dots, x_n] \to \mathbb{B}$. Note that ϕ can only send every invertible element of A to 1, for otherwise the image of ϕ is 0. Hence ϕ is defined in the following way,

$$0_A \mapsto 0, and\ A \setminus 0_A \mapsto 1$$
$$x_i \mapsto 1, for\ i \in I \subseteq \{1, \dots, n\}$$
$$x_j \mapsto 0, for\ j \in \{1, \dots, n\} \setminus I.$$

Denote by P the kernel of ϕ. Note that P is a prime congruence and $A[x_1, \dots, x_n]/P \cong \mathbb{B}$. Furthermore the kernel of P is a saturated ideal by definition, but it is also prime since P is prime. The map ϕ is completely determined by the choice of the set I and hence there are 2^n such maps.

Now we want to see that every saturated prime ideal determines a maximal congruence. For the saturated prime ideal $\mathfrak{a}$ of $A[x_1, \dots, x_n]$, consider the congruence $P_{\mathfrak{a}}$, generated by the pairs $(a, 0)$, for $a \in \mathfrak{a}$ and $(u, 1)$, for $u \notin \mathfrak{a}$. Note that this is a proper congruence with quotient $\mathbb{B}$ and hence it is prime and maximal. □

We proceed to describe the congruences of $\mathbb{T}[\boldsymbol{x}]$ with quotient $\mathbb{T}$ and understand their role in the context of the Nullstellensatz problem. First note that if $\boldsymbol{a} = (t^{d_1}, \dots, t^{d_k}) = t^{\boldsymbol{d}}$ is a point in $\mathbb{T}^k$ such that all of its coordinates are non-zero and $m = t^c \boldsymbol{x}^{\boldsymbol{n}}$ is a monomial in $\mathbb{T}[\boldsymbol{x}]$, then $m(\boldsymbol{a}) = t^{c + \sum_i (d_i n_i)} = t^{(c, \boldsymbol{n})(1, \boldsymbol{d})}$. Hence $\mathbb{E}(\{\boldsymbol{a}\}) = P[U]_{\mathbb{T}}$ for the matrix U consisting of the single row $(1, d_1, \dots, d_k)$. Similarly, when some of the coordinates of $\boldsymbol{a}$ are zero $Ker(\mathbb{E}(\{\boldsymbol{a}\})$ will be generated by the variables corresponding to the zeros of $\boldsymbol{a}$, and $\mathbb{E}(\{\boldsymbol{a}\})$ restricted to the rest of the variables will be defined by the matrix whose single row is $(1, d'_1, \dots, d'_i)$, where the $d'_1, \dots, d'_i$ are the exponents of the non-zero entries of $\boldsymbol{a}$. We will call the congruences $\mathbb{E}(\{\boldsymbol{a}\})$ *geometric congruences.* Note that these are precisely the congruences whose quotient is $\mathbb{T}$.

Remark 6.2.2. *It is important to note that $\mathbb{E}(\mathbb{V}(C))$ is the intersection of all geometric congruences lying above C, because $v \in \mathbb{V}(C)$ if and only if C is contained in the geometric congruence $Ker(\varphi_v)$, where $\varphi_v : \mathbb{T}[\boldsymbol{x}] \to \mathbb{T}$ is the evaluation morphism at the point v.*

6.3 The Tropical Nullstellensatz

We will need the following proposition:

Proposition 6.3.1. *(i) For a $\mathbb{B}$-algebra A, a pair $\alpha \in A \times A$ and a congruence C with $GP(\alpha) \cap C \neq \emptyset$, there is a non-negative integer i and an element $h \in A$ such that $(\alpha^{*i} + (h,0))\alpha \in C$.*

(ii) For a congruence C of $\mathbb{T}[\boldsymbol{x}]$ and any $\epsilon \in \mathbb{T} \setminus \{1,0\}$ we have that

$$C_+ = \{(f,g) \in \mathbb{T}[\boldsymbol{x}] \times \mathbb{T}[\boldsymbol{x}] | \; GP((1,\epsilon)(f,g)) \cap C \neq \emptyset\} = \{(f,g) \mid \; (f,g)(1,\epsilon) \in Rad(C)\}.$$

Proof. For (i), if $GP(\alpha) \cap C \neq \emptyset$, then by definition we have non-negative integers i,j and a $h \in A$ such that $\beta := (\alpha^{*i} + (h,0))\alpha^j \in C$. If $j \leq 1$ we are done, let us assume $j > 1$. After expanding, we obtain that in the quotient A/C we have

$$\alpha_1^{i+j} + h\alpha_1^j \leq \beta_1 = \beta_2 \leq \sum_{s=1}^{s=i+j} \alpha_1^{i+j-s}\alpha_2^s + h\sum_{s=1}^{s=j} \alpha_1^{j-s}\alpha_2^s.$$

Now set $h' = h(\alpha_1 + \alpha_2)^{j-1}$ and $\gamma := (\alpha^{*i+j-1} + (h',0))\alpha$. After expanding the parenthesis, we obtain:

$$\gamma_1 = \sum_{s=1}^{s=i+j} \alpha_1^s\alpha_2^{i+j-s} + h\sum_{s=1}^{s=j} \alpha_1^s\alpha_2^{j-s}$$

$$\gamma_2 = \sum_{s=1}^{s=i+j} \alpha_1^{i+j-s}\alpha_2^s + h\sum_{s=1}^{s=j} \alpha_1^{j-s}\alpha_2^s$$

We see that the only terms appearing in γ_1 but not in γ_2 are α_1^{i+j} and $h\alpha_1^j$, so comparing with the previous inequality we obtain that in the quotient A/C we have $\gamma_2 \geq \gamma_1$ and then by a symmetric argument $\gamma_2 = \gamma_1$, hence $\gamma \in C$.

For (ii) first note that a prime congruence contains the pair $(1,\epsilon)$ for an $\epsilon \in \mathbb{T} \setminus \{1,0\}$ if and only if its defining matrix has all zero entries in the first column. Now by Proposition 3.2.12 the set $F := \{(f,g) \in \mathbb{T}[\boldsymbol{x}] \times \mathbb{T}[\boldsymbol{x}] | \; GP((1,\epsilon)(f,g)) \cap C \neq \emptyset\}$ is the intersection of the prime congruences containing C but not containing $(1,\epsilon)$ so by the previous comment it does not depend on the choice of ϵ. Furthermore we have

$$(1,\epsilon)((f,g)^{*i} + (h,0))(f,g) \in GP((1,\epsilon)(f,g))$$

hence $C_+ \subseteq F$. For the other inclusion if $(f,g) \in F$ then by (i) we have an integer i and a $h \in \mathbb{T}[\boldsymbol{x}]$

such that

$$((1,\epsilon)^{*i}(f,g)^{*i} + (h,0))(1,\epsilon)(f,g) \in C.$$

Now since $(1+\epsilon)$ has a multiplicative inverse for any $\epsilon \in \mathbb{T}$, after multiplying the above expression with $1/(1+\epsilon)^i$ we obtain that $(f,g) \in C_+$. The second equality follows from Proposition 3.2.12. □

We will denote the i-th row of the matrix U by $U[i]$. For an $l \times k$ admissible (resp. z-admissible, t-admissible) matrix U and a vector $\boldsymbol{w} = (w_1, \dots, w_l) \in \mathbb{R}_+^l$, $P[\boldsymbol{w}U]$ (resp. $P[\boldsymbol{w}U]_{\mathbb{Z}_{max}}$, $P[\boldsymbol{w}U]_{\mathbb{T}}$) will denote the prime defined by the matrix consisting of the single row $\boldsymbol{w}U = \sum_i w_i U[i]$. Note that since the coefficients w_i are positive and the rows of an admissible matrix are linearly independent $\boldsymbol{w}U$ will be also admissible (resp. z-admissible, t-admissible). The following lemma holds by identical arguments over all polynomial and Laurent polynomial semirings we have studied so far, to simplify its formalization we will denote by $P(U)_*$ one of $P(U)$, $P[U]$, $P(U)_{\mathbb{Z}_{max}}$, $P[U]_{\mathbb{Z}_{max}}$, $P(U)_{\mathbb{T}}$ or $P[U]_{\mathbb{T}}$ depending on which semiring is being considered.

Lemma 6.3.2. *Let $P(U)_*$ be a prime with trivial kernel in one of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$, $\mathbb{B}[\boldsymbol{x}]$, $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$, $\mathbb{Z}_{max}[\boldsymbol{x}]$, $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ or $\mathbb{T}[\boldsymbol{x}]$. Then for any pair (f,g) we have that $(f,g) \in P$ if and only if there exist positive real numbers $r_1, \dots, r_{l-1}$ such that for any $\boldsymbol{w} \in \mathbb{R}_+^l$ satisfying $w_i/w_{i+1} > r_i$ $(\forall i : 1 \le i \le l-1)$, we have $(f,g) \in P(\boldsymbol{w}U)_*$.*

Proof. We will prove the proposition for polynomials in $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$ and note that it holds by identical arguments for all of the semirings listed. Let $f = \sum_i \boldsymbol{x}^{\boldsymbol{n}_i}$ a polynomial in $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$, and recall that since the quotient of any prime is totally ordered f will be congruent in any prime to one or more of its monomials. Now it is easy to verify that if we pick r_i large enough then for any w satisfying $w_i/w_{i+1} > r_i$ for all $1 \le i \le l-1$ and any $\boldsymbol{n}_i, \boldsymbol{n}_j$ appearing as exponents in f we have that $\boldsymbol{w}U\boldsymbol{n}_i \ge \boldsymbol{w}U\boldsymbol{n}_j$ if and only if either $U\boldsymbol{n}_i = U\boldsymbol{n}_j$ or for the smallest s such that $U[s]\boldsymbol{n}_i \neq U[s]\boldsymbol{n}_j$ we have $U[s]\boldsymbol{n}_i > U[s]\boldsymbol{n}_j$. It follows that for large enough r_i-s and a $\boldsymbol{w}$ as in the proposition, the leading terms of both f and g in $P(\boldsymbol{w}U)$ are the same as in $P(U)$, hence $(f,g) \in P(U)$ if and only if $(f,g) \in P(\boldsymbol{w}U)$. □

Theorem 6.3.3. *(i) For a finitely generated congruence C in one of $\mathbb{B}[\boldsymbol{x}^{\pm 1}]$, $\mathbb{B}[\boldsymbol{x}]$, $\mathbb{Z}_{max}[\boldsymbol{x}^{\pm 1}]$, $\mathbb{Z}_{max}[\boldsymbol{x}]$, $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ or $\mathbb{T}[\boldsymbol{x}]$, we have that $Rad(C)$ is the intersection of the primes that contain C and have a quotient of dimension at most 1.*

(ii) In $\mathbb{T}[\boldsymbol{x}]$, for any finitely generated congruence C, we have $C_+ = \mathbb{E}(\mathbb{V}(C))$.

Proof. For (i) let C be a congruence generated by the pairs $\{(f_1, g_1), \dots, (f_s, g_s)\}$. By definition we have that $Rad(C) = \cap\{P \mid \text{P prime}, (f_i, g_i) \in P\ \forall i\}$. If $P(U)_*$ is a prime with trivial kernel and a quotient of dimension $l \geq 2$, containing all of the (f_i, g_i) then we can choose $(r_1, \dots, r_{l-1})$ that are large enough for all of the (f_i, g_i) in the setting of Proposition 6.3.2. Denoting by W the set of vectors $\boldsymbol{w} \in \mathbb{R}^l_+$ satisfying $w_i/w_{i+1} > r_i$ for all $1 \leq i \leq l-1$, it follows that $(f_i, g_i) \in P(\boldsymbol{w}U)_*$ for all $1 \leq i \leq s$ and $\boldsymbol{w} \in W$. Moreover by applying the other direction of Proposition 6.3.2 we also have that $\cap_{\boldsymbol{w}\in W} P(\boldsymbol{w}U)_* \subseteq P(U)_*$, hence $P(U)_*$ can be removed from the intersection defining $Rad(C)$. We can argue the same way in the case when $P(U)_*$ has non-trivial kernel by considering it in the polynomial subsemiring generated by the variables that are not in $Ker(P(U)_*)$.

For (ii) by Proposition 6.3.1 and Proposition 3.2.12 we have that C_+ is the intersection of the primes that contain C but not contain $(1, \epsilon)$ for any $\epsilon \in \mathbb{T} \setminus \{1\}$, and by the discussion at the start of this section it follows that $\mathbb{E}(\mathbb{V}(C))$ is the intersection of the geometric congruences containing C, which are exactly those primes that have quotients with dimension 1 and not contain the pair $(1, \epsilon)$ for any $\epsilon \in \mathbb{T} \setminus \{1\}$. Note that $(1, \epsilon)$ for $\epsilon \in \mathbb{T} \setminus \{1\}$ is contained in a prime precisely when its defining matrix has all zeros in the first column, thus if $(1, \epsilon) \notin P[U]_{\mathbb{T}}$ then $(1, \epsilon) \notin P[\boldsymbol{w}U]_{\mathbb{T}}$ for any vector $\boldsymbol{w}$ with positive entries. Now one can argue the same way as for (i). □

Without the assumption on the finite generation of the congruence C the above statement is not necessarily true as could be seen in the following example.

Example 6.3.4. Set C to be the congruence of $\mathbb{T}[x]$ generated by the pairs $(t^{-c} + x, x)$ for all $c > 0$. Then notice that $(1 + x, x)$ is not in C and moreover it is not in $Rad(C)$. To see this, consider the prime P with defining matrix

$$U = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then $C \subset P$ since in $\mathbb{T}[x]/P$ we have that $t^{-c} \leq x$, but $(1 + x, x) \notin P$.

Now let $C \subset P'$, where P' is a rank one prime, that is, there exists a 1×2 matrix U', such that $P' = P[U']$. Then it is easy to see that $(1 + x, x) \in P'$ and hence in the intersection of all primes of rank at most 1.

We conclude this section with a statement showing that the polynomials that agree on every point of $\mathbb{T}^k$ are precisely the pairs that are in $Rad(\Delta)$. This is essentially the same as Theorem 1 of [BE13], but our proof is different.

Proposition 6.3.5. $\mathbb{E}(\mathbb{T}^k) = \Delta_+ = Rad(\Delta)$.

Proof. The first equality follows from Theorem 6.3.3. For the second equality since Δ_+ is the intersection of a subset of all primes we clearly have $Rad(\Delta) \subseteq \Delta_+$. For the other inclusion, if $(f, g) \notin Rad(\Delta)$ then by Theorem 5.3.4 we have that for one of them, say f, there is a vertex v on $\overline{newt(f)}$ that lies outside of $\overline{newt(g)}$. Now by the same argument as in the proof of Theorem 5.2.1 one can pick a vector $\boldsymbol{u}$ with positive first entry such that v is the unique vertex that maximizes the scalar product taken with $\boldsymbol{u}$ on $\overline{newt(f)}$. Now let U be a t-admissible matrix with $\boldsymbol{u}$ as its first row such that $P[U]_{\mathbb{T}}$ is a minimal prime. Since in $P(U)_{\mathbb{T}}$ each equivalence class contains precisely one monomial and f is congruent to the monomial with exponent v we have $(f, g) \notin P[U]_{\mathbb{T}}$. Moreover since the first entry of $\boldsymbol{u}$ is nonzero $(1, \epsilon) \notin P[U]_{\mathbb{T}}$ for any $\epsilon \in \mathbb{T} \setminus \{1\}$. Now since by Proposition 6.3.1 and Proposition 3.2.12 Δ_+ is the intersection of all primes that do not contain $(1, \epsilon)$ for $\epsilon \in \mathbb{T} \setminus \{1\}$, we have that $\Delta_+ \subseteq P[U]_{\mathbb{T}}$ and consequently $(f, g) \notin \Delta_+$. □

6.4 On the Weak Nullstellensatz

In this chapter we discuss the tropical weak Nullstellensatz.

It was originally proven in Theorem 2 of [BE13], but here we show how the statement follows from our theory. The weak Nullstellensatz answers the question when the set $\mathbb{E}(\mathbb{V}(C))$ is empty if C is a finitely generated congruence. We show that $\mathbb{E}(\mathbb{V}(C)) = \emptyset$ if and only if there exists a polynomial $h \in \mathbb{T}[\boldsymbol{x}]$ with nonzero constant term such that $(h, \epsilon h) \in C$ for some $\epsilon \in \mathbb{T}$.

A recent result presents a different formulation of the weak Nullstellensatz cf. Theorem 8 in [GP14] stated in terms of the lack of solution to a system of polynomial equations of degree no higher than a certain number. The part of the theorem concerning the existence of a solution can be regarded as a special case of our work.

The following proposition can be regarded as a weak Nullstellensatz,

Proposition 6.4.1. *Consider a finitely generated congruence C, of $\mathbb{T}[\boldsymbol{x}]$ or $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ then $(1, \epsilon) \in Rad(C)$ if and only if $\mathbb{V}(C) = \emptyset$.*

Proof. Recall that $\mathbb{E}(\mathbb{V}(C)) = C_+ = \{(f, g) | (f, g)(1, \epsilon) \in Rad(C)\}$, hence $(1, \epsilon) \in Rad(C)$ if and only if $\mathbb{E}(\mathbb{V}(C)) = \mathbb{T}[\boldsymbol{x}] \times \mathbb{T}[\boldsymbol{x}]$ or equivalently $\mathbb{V}(C) = \emptyset$. □

Remark 6.4.2. If $(1, \epsilon) \in Rad(C)$, then by Proposition 6.3.1 (i) there exist k and h such that $((1, \epsilon)^k)^* + (h, 0))(1, \epsilon) \in C$. Without loss of generality we assume that $1 > \epsilon$. We can do this because of the following observation. If $(1, \epsilon) \in Rad(C)$ then so does the product $(1/\epsilon, 0)(1, \epsilon) = (1/\epsilon, 1)$. Furthermore, either $\epsilon < 1$ or $1/\epsilon < 1$. With this assumption we obtain that if $(1, \epsilon) \in Rad(C)$ then

$(1+h, \epsilon + \epsilon h) \in C$. However, by Proposition 6.4.1 $(1, \epsilon) \in Rad(C)$ implies that $\mathbb{V}(C) = \emptyset$, which is exactly the weak Nullstellensatz theorem from [BE13].

We recall some definitions from [GP14], which reformulate for the max-plus case. A point $\boldsymbol{a} \in \mathbb{T}^k$ *root of a polynomial* $f \in \mathbb{T}[\boldsymbol{x}]$ if the maximum of $f(\boldsymbol{a})$ is attained on at least two monomials or is $-\infty$. A point $\boldsymbol{a} \in \mathbb{T}^k$ *root of a pair* of polynomials $f(\boldsymbol{x}) = g(\boldsymbol{x})$, for $f, g \in \mathbb{T}[\boldsymbol{x}]$ if $f(\boldsymbol{a}) = g(\boldsymbol{a})$.

An *algebraic combination* denoted by $f = g$ or (f, g) of a set of polynomials $F = \{f_1 = g_1, \dots, f_k = g_k\}$ over $\mathbb{T}[\boldsymbol{x}]$ is an element of the smallest ideal I of $\mathbb{T}[\boldsymbol{x}] \times \mathbb{T}[\boldsymbol{x}]$, which contains F, Δ and is symmetric, that is $(m, n) \in I$ implies $(n, m) \in I$. Note that the multiplication operation here is the usual coordinate-wise multiplication and not the twisted product.

We now recall the existence part of Theorem 8 from [GP14]. Consider a system of polynomials $F = \{f_1 = g_1, \dots, f_k = g_k\}$ over $\mathbb{T}[\boldsymbol{x}]$. Over the semiring $\mathbb{T} \setminus \{-\infty\}$ the system F has no solution if and only if we can construct an algebraic combination $f = g$, where $f, g \in \mathbb{T}[\boldsymbol{x}]$ such that for each monomial M its coefficient in f is greater than its coefficient in g. Over $\mathbb{T}$, F has no solution if the same condition holds with the extra condition that the constant term of g is finite.

Remark 6.4.3. *Given a system of polynomials $F = \{f_1 = g_1, \dots, f_k = g_k\}$, the solutions of F are the same as the points of $\mathbb{V}(C)$, where C is the congruence generated by the elements of F.*

Here we restate the Theorem 8 from [GP14] using the formalism of this thesis.

Theorem 6.4.4. *Let C be the congruence generated by $\{(f_1, g_1), \dots, (f_k, g_k)\}$. Then*

a) F has no solution over $\mathbb{T} \setminus \{-\infty\}$, equivalently $\mathbb{V}(C)$ is empty if and only if there is a pair (f, g) which is an algebraic combination of the generators, such that every coefficient in f is bigger than the corresponding coefficient in g. (i.e. $\overline{newt(f)}$ is sitting over $\overline{newt(g)}$).

b) F has no solution over $\mathbb{T}$, if and only if there is a pair (f, g) which is an algebraic combination of the generators, such that every coefficient in f is bigger than the corresponding coefficient in g and g has a constant term.

We would need the following lemma for the proof of the theorem.

Lemma 6.4.5. *Let (f, g) be a pair of polynomials over $\mathbb{T}[\boldsymbol{x}^{\pm 1}]$ or $\mathbb{T}[\boldsymbol{x}]$, such that the coefficient of every monomial of f is bigger than the coefficient of the corresponding monomial of g. Then for any polynomial h the pair $h(f, g)$ satisfies the same condition on the coefficients.*

Proof. Follows from straightforward computation and the observation that the multiplication of the coefficients is usual addition. □

We would also like to make the following observation.

Lemma 6.4.6. *Let C be a congruence generated by the pairs $(f_1, g_1), \ldots, (f_k, g_k)$. If α is in C then for some non-zero h, the pair $(h, 0)\alpha$ is algebraically generated by the pairs (f_i, g_i), for $1 \leq i \leq k$.*

Proof. The only part that is not obvious is the transitivity. Consider two pairs of polynomials (a, b) and (b, c). Then the pair obtained by coordinate-wise multiplication $(a, b)(b, c) = (ab, bc) = (b, 0)(a, c) = b(a, c)$ is algebraically generated by (a, b) and (b, c), even though (a, c) might not be. □

We are now ready to prove Theorem 6.4.4.

Proof. We will treat both cases at the same time. In the first case, when we are looking for solutions over $\mathbb{T}$, the condition on g ensures that even if every coefficient of f is bigger than the corresponding coefficient of g there is no $\boldsymbol{a} \in \mathbb{T}^n$ such that $f(\boldsymbol{a}) = g(\boldsymbol{a}) = -\infty$.

First we show that if there exists a pair (f, g) with the desired property then $\nexists\ \boldsymbol{a} \in \mathbb{T}^n$ such that $f(\boldsymbol{a}) = g(\boldsymbol{a})$ and so we always have $f(\boldsymbol{a}) > g(\boldsymbol{a})$ or $f(\boldsymbol{a}) < g(\boldsymbol{a})$. Without loss of generality we can assume that f and g have the same monomials all with non-zero coefficients, because we can always add to (f, g) a pair from the diagonal, that is of the form (h, h) keeping the condition on the coefficients and the algebraic generation. Note that we can also assume without loss of generality that all coefficients are positive by multiplying (f, g) with pairs of the form $(k, 0)$ for large enough positive k. Thus if $f = \sum c_i M_i$, where M_is are monomials and $g = \sum b_i M_i$, $f(\boldsymbol{a}) = \max(c_i + M_i(\boldsymbol{a}))$ and $g(\boldsymbol{a}) = \max(b_i + M_i(\boldsymbol{a}))$. Hence we see that if $c_i > b_i$ for every i, then $f(\boldsymbol{a}) > g(\boldsymbol{a})$.

For the other direction, if $\mathbb{V}(C) = \emptyset$, then show there is a pair (f, g) which satisfies the conditions in the proposition. However from Proposition 6.4.1 follows that if $\mathbb{V}(C) = \emptyset$, then $(1, \epsilon) \in Rad(C)$ and hence $(f, \epsilon f) \in C$, for some f with a non-zero constant term. Depending on ϵ either f or ϵf has bigger coefficients, i.e. $\overline{newt(f)}$ is sitting over $\overline{newt(\epsilon f)}$ (or the other way around). Note that even though this pair satisfies the condition on the coefficients it $(f, \epsilon f)$ may not be an algebraic combination of the set F, that is it is in the transitive closure of (all algebraic combinations of) F. But by Lemma 6.4.5 and the observation following it we can take instead a pair $h(f, \epsilon f)$ for some h which has all desired properties. □

7

Connections to tropical varieties

In this chapter we describe how the results obtained in the previous sections relate to the existing notions of tropical varieties and tropical schemes introduced in Chapter 2.

For the rest of this section K will be a field with a valuation $\nu : K \to \mathbb{T}$ and $(K^*)^n$ will be the n-dimensional torus over K.

7.1 Bend relations and set theoretic tropicalization

We start with a remark on our notation. We would use $V(I)$ to denote the zero locus of an ideal I and $\mathbb{V}(C)$ to be the set defined in the previous section $\mathbb{V}(C) = \{\boldsymbol{w} \in \mathbb{T}^k \mid f(w) = g(w), \forall (f, g) \in C\}$, for a congruence C. This should not lead to ambiguity.

We make an observation that links set-theoretic tropicalization, tropical schemes and the sets $\mathbb{V}(C)$ defined in the previous section. Let I be an ideal of $K[x^{\pm 1}]$ and let $X = V(I)$, then

$$\mathbb{V}(Bend(I)) = trop(X). \tag{7.1.1}$$

This equality follows directly from the definition of the above objects. Recall that $Bend(I) = \{(\nu(f), \nu(f)_{\hat{i}}) \ : \ \forall f \in I\}$, then $\mathbb{V}(Bend(I)) = \{\boldsymbol{w} \ : \ \nu(f)(\boldsymbol{w}) = \nu(f)_{\hat{i}}(\boldsymbol{w}), \forall f \in I\} = \{\boldsymbol{w} \ : \ trop(f)(\boldsymbol{w}) = trop(f)_{\hat{i}}(\boldsymbol{w})\}$. In other words $\mathbb{V}(Bend(I))$ is the set of all points for which every $f \in I$, $trop(f)(\boldsymbol{w})$ achieves its maximum twice or alternatively the initial ideal $in_{\boldsymbol{w}} I$ does not contain 1. This set is $trop(X)$ by Theorem 2.1.9.

Remark 7.1.1. *Notice that if $X = V(I)$, then every point $\boldsymbol{w}$ on $trop(X)$ corresponds to a geometric prime congruence which lies above $Bend(I)$ and has defining matrix $[1 \ \boldsymbol{w}]$.*

Let I be an ideal of $K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, where K a valued field, and let I be generated by $\{f_1, \ldots, f_k\}$. We saw in Example 2.2.3 that the bend congruence $Bend(I)$ of an ideal may not be determined by the generators of I, in fact this is rarely the case even for principal ideals. In other words $Bend(f) \subsetneq Bent(I)$.

Remark 7.1.2. This strict containment be seen even in the simplest case, for example when $f = x+y+z$. It is easy to show that the relation $x^2+xy+y^2 \sim x^2+xy+y^2+yz$ belongs to $Bend(\langle f \rangle)$ but not to $Bend(f)$.

Remark 7.1.3. Note that even if we consider the polynomials as functions that is, consider $Bend(I)$ over the $Rad(\Delta)$, then we still have $\langle Bend(f), Rad(\Delta)\rangle \subsetneq \langle Bend(I), Rad(\Delta)\rangle$. We can see this in the following example.

Example 7.1.4. Similarly to Example 2.2.3, let $f = x^3 + x^2y + xy^2 + y^3$ and $I = \langle f \rangle$. Then the bend relations in degree 3 are generated by

$$x^2y + xy^2 + y^3 \sim x^3 + xy^2 + y^3 \sim x^3 + x^2y + y^3 \sim x^3 + x^2y + xy^2.$$

Now if we look at the congruence over $Rad(\Delta)$ we see that in degree 3 the bend relations are generated by

$$x^3 + y^3 \sim x^3 + xy^2 \sim x^2y + y^3.$$

However in degree 4, we have $x^4 \sim y^4$, since $(x-y)f \in I$, but (x^4, y^4) is not in the semi-module congruence $\langle Bend(f), Rad(\Delta)\rangle$.

However, we have the following (non-surprising) result.

Proposition 7.1.5. *Let I be and ideal of $K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ such that $I = \langle f \rangle$, then*

$$\mathbb{V}(Bend(f)) = \mathbb{V}(Bend(I)).$$

Proof. First note that $\mathbb{V}(Bend(f)) = \{\boldsymbol{w} \in \mathbb{T}^n : f(\boldsymbol{w}) = f_{\hat{i}}(\boldsymbol{w})\}$, in other words this is the set of points in $\mathbb{T}$ for which the maximum of f is achieved at least twice. But this means that $\mathbb{V}(Bend(f)) = trop(V(I))$ by definition of a tropical hypersurface. On the other hand, by (7.1.1) we have that $\mathbb{V}(Bend(I)) = trop(V(I))$, hence the statement. □

We know that by Theorem 2.1.7 and Corollary 2.1.8 every tropical variety is determined by a finite set of polynomials, namely its tropical basis. In particular, if an ideal is principal then its generators is a tropical basis. We can generalize the above result.

Let I be an ideal of $K[\boldsymbol{x}^{\pm 1}]$ with tropical basis $\mathcal{T}$. We will denote by $Bend(\mathcal{T})$ the congruence generated by the bend relations of the coefficient-wise valuations of the elements of $\mathcal{T}$.

Proposition 7.1.6. *Let I be an ideal of the Laurent polynomial ring over K. Then there exists a finite subset $G \subset Bend(I)$ such that $\mathbb{V}(G) = \mathbb{V}(Bend(I))$, namely $G = Bend(\mathcal{T})$, where $\mathcal{T}$ is a tropical basis for I.*

Proof. Let $G = Bend(\mathcal{T})$. Since $G \subseteq Bend(I)$ then $\mathbb{V}(G) \supseteq \mathbb{V}(Bend(I))$. We need to show the opposite inclusion. Assume $\boldsymbol{w'} \notin \mathbb{V}(Bend(I))$, we want to see that $\boldsymbol{w'} \notin \mathbb{V}(G)$. Recall that $\mathbb{V}(Bend(I)) = trop(X) = \{\boldsymbol{w} : in_{\boldsymbol{w}} I \neq \langle 1 \rangle\}$, so $\boldsymbol{w'}$ is such that $in_{\boldsymbol{w'}} I = \langle 1 \rangle$, but then by definition of tropical basis this means that $in_{\boldsymbol{w'}} \mathcal{T} = \langle 1 \rangle$, then $\boldsymbol{w'} \notin \mathbb{V}(G)$, which means that $trop(f)(w)$ achieves its maximum only once for some $f \in \mathcal{T}$. □

Remark 7.1.7. Note that $Bend(I)$ is almost never finitely generated and thus usually $G \subsetneq Bend(I)$.

Remark 7.1.8. If C is any non-finitely generated congruence, then there does not necessarily exist a finite set G such that $\mathbb{V}(G) = \mathbb{V}(C)$. It can be seen in the following example.

Example 7.1.9. Recall from Example 6.3.4 the congruence C of $\mathbb{T}[x]$ generated by the pairs $(t^{-c} + x, x)$ for all $c > 0$. Note that

$$\mathbb{V}(C) = \{t^c : \ c \geq 0\} = [1, \infty).$$

To see this, note that $\mathbb{V}(C) = \bigcap_{(f,g) \in C} V(f,g)$, where $V(f,g) = \{a : \ f(a) = g(a)\}$. We obtain that

$$\mathbb{V}(C) = \bigcap_{(f,g) \in C} V(f,g) = \bigcap_{c>0} \{a : \ t^{-c} \leq a\} = \bigcap_{c>0} [t^{-c}, \infty) = [1, \infty).$$

Now let G be a finite subset of C, of cardinality $g < \infty$. Assume that $\mathbb{V}(G) = \mathbb{V}(C)$, then $\mathbb{V}(G) = [1, \infty)$. But

$$\mathbb{V}(G) = \bigcap_{(f,g) \in G} V(f,g) = \bigcap_{c>0}^{g} [t^{-c}, \infty) = [1, \infty),$$

but since this is a finite intersection if intervals ($g < \infty$), then one of the intervals is $[1, \infty)$, which means that one of the pairs in G is $(1 + x, x)$, but this is a contradiction because $(1 + x, x) \notin C$ as seen in Example 6.3.4.

7.2 Krull dimension of tropical varieties

Recall that by Theorem 2.1.10 the tropicalization $trop(X)$ of a d-dimensional subvariety X of $(K^*)^n$ is a polyhedral complex of pure dimension d. The goal of this section is to relate the dimension of X or rather $trop(X)$ to the Krull dimension that we have defined in Chapter 3.

Theorem 7.2.1. *Let $X = V(I)$ be a subvariety of $(K^*)^n$ of dimension d. Then*

$$\dim \mathbb{T}[\boldsymbol{x}]/Bend(I) = d + 1.$$

Proof. We begin by making the following observation. Let C be a congruence, then $\dim \mathbb{T}[\boldsymbol{x}]/C = \dim \mathbb{T}[\boldsymbol{x}]/P$, where P is a prime over C of maximal rank. If P has a defining matrix U of rank $r(U)$, then recall that by Proposition 5.3.3 we have that $\dim \mathbb{T}[\boldsymbol{x}]/P = r(U)$. Thus if P is a maximal rank prime over $Bend(I)$, it suffices to show that P has rank $d + 1$.

We first see that there always exists a prime P with defining matrix U containing $Bend(I)$, such that P has a geometric prime lying over it and has rank $r(U) = d + 1$. Let $\mathcal{F}$ be a maximal cell of the polyhedral complex $trop(X)$ and $\omega \in \mathcal{F}$. Now the affine span of $\mathcal{F}$ has dimension equal to the dimension of $trop(X)$ which is d. Hence, there exist d vectors $u_1, \dots, u_d$ such that $\omega, u_1, \dots, u_d$ are affine independent and $in_\omega I = in_{\omega+u_1\epsilon_1} I = \cdots = in_{\omega+u_1\epsilon_1+\cdots+u_d\epsilon_d} I$, for ϵ_i small enough. Now consider the matrix

$$U = \begin{bmatrix} 1 & \omega \\ 1 & \omega + u_1\epsilon_1 \\ \vdots & \vdots \\ 1 & \omega + u_1\epsilon_1 + \cdots + u_d\epsilon_d \end{bmatrix}.$$

Since $\omega, u_1, \dots, u_d$ are affine independent then the rows of U are linearly independent and thus $r(U) = d + 1$. Furthermore, we can choose ϵ_i, for $1 \leq i \leq d$ suitably so that U is admissible. Hence it is the defining matrix of a prime congruence, which we will call P. Notice that P contains $Bend(I)$, since if $v \in trop(X)$ then every polynomial of I takes its maximum twice with respect to the vector $(1, v)$.

We remain to see that every prime P over $Bend(I)$ has rank at most $d + 1$. We first show this in the case when P has a geometric prime over it. Assume for contradiction that P is such a prime over $Bend(I)$. Let W be the defining matrix of P of rank $r(W) > d + 1$. Denote the rows of W by $w_1, \dots, w_{r(W)}$. Note that they are linearly independent by definition. Consider the vectors $w'_1 = w_1,\ w'_2 = w_1 + \epsilon'_1 w_2,\ \dots,\ w'_{r(W)} = w_1 + \cdots + \epsilon'_{r(W)} w_{r(W)}$ which are also linearly independent.

We can scale each of the vectors $w'_1, \dots, w'_{r(W)}$ so that the first entry is 1. Now consider the rescaled vectors without the first entry and call them $w''_1, \dots, w''_{r(W)}$. Note that the vectors $w''_1, \dots, w''_{r(W)}$ are affine independent and lie on the same face of $trop(X)$. Since we know that the dimension of $trop(X)$ is at most d, we know that $r(W) \leq d+1$.

Remains to investigate the case when P (containing $Bend(I)$) does not have a geometric prime over it. Let the matrix of P be U. By assumption the first entry of the first row is zero. However, if the first entry of any other row is not zero, we can add a suitable multiple of this row to the first one. This way we obtain the matrix of a different prime of the same rank, which still contains $Bend(I)$ but has a geometric prime over it. We are done by the previous discussion. So we can assume that the entries in first column of U are all zeroes. Now consider the prime P' with matrix U', where

$$U' = \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & U \end{bmatrix}.$$

Then there are two cases. First if the valuation ν is trivial, then prime P' lies above $Bend(I)$ and clearly $r(U') > r(U)$. So P is not a maximal rank prime over $Bend(I)$. Now, let ν be non-trivial. Consider the prime P' as before and notice that since it is a prime over $Bend(I)$ when ν is trivial, and since there is a geometric prime over P', then by the earlier argument $\dim \mathbb{T}[\boldsymbol{x}]/P'$ is at most $\dim X + 1$, that is at most $d+1$. Now since $r(U') > r(U)$, then $r(U) < d+1$ and hence is not a maximal rank prime. So we conclude that if P is a maximal rank prime with matrix U, then $r(U) = d+1$. □

7.3 Bend congruences and higher rank primes

We begin by pointing the reader's attention to the fact that

$$trop(V(I)) = Hom(\mathbb{T}[\boldsymbol{x}]/Bend(I), \mathbb{T}).$$

In this section we investigate the answer to the following question. Can we find two different congruences C, C' such that $Hom(\mathbb{T}[\boldsymbol{x}]/C, \mathbb{T}_n) = Hom(\mathbb{T}[\boldsymbol{x}]/C', \mathbb{T}_n)$? Recall that we denote by $\mathbb{T}_n$ the semifield with underlying set $\mathbb{R}^n \cup \{-\infty\}$, with multiplication being the usual vector addition and addition defined so it induces the lexicographic ordering on the base set.

Proposition 7.3.1. *Let R and S be two semirings and let S be a domain. Let $\phi : R \to S$ be a semiring homomorphism. Then* $\ker \phi$ *is prime.*

Proof. $\operatorname{Im}\phi \simeq R/\ker\phi$. But $\operatorname{Im}\phi$ is a subsemiring of S hence also a domain. Therefore $\ker\phi$ is prime by Proposition 4.2 (ii) □

Note that $\mathbb{T}_n$ is a domain, since it is quotient cancellative and totally ordered by Proposition 3.1.14. Thus if $\phi : \mathbb{T}[\boldsymbol{x}] \to \mathbb{T}_n$ then $\ker\phi$ is prime by Proposition 7.3.1.

Consider the set $Hom(\mathbb{T}[\boldsymbol{x}]/C, \mathbb{T}_n)$. It is the set of morphisms ϕ from $\mathbb{T}[\boldsymbol{x}]$ to $\mathbb{T}_n$, such that $\ker\phi \supseteq C$. In general, $Hom(\mathbb{T}[\boldsymbol{x}]/C, \mathbb{T}_n) = Hom(\mathbb{T}[\boldsymbol{x}]/Rad(C), \mathbb{T}_n)$ thus we only need to consider the case where C and C' are radical congruences, because by the above discussion $\ker\phi$ is a prime congruence over C for every $\phi \in Hom(\mathbb{T}[\boldsymbol{x}]/C, \mathbb{T}_n)$ and $Rad(C)$ is the intersection of all prime congruences lying over C.

Proposition 7.3.2. *In the case when $n = 1$ and C and C' are finitely generated congruences $Hom(\mathbb{T}[\boldsymbol{x}]/C, \mathbb{T})$ is completely determined by C_+. In particular $Hom(\mathbb{T}[\boldsymbol{x}]/C, \mathbb{T}) = Hom(\mathbb{T}[\boldsymbol{x}]/C', \mathbb{T})$ if and only if $C_+ = C'_+$.*

Proof. By definition C_+ is the set of all primes that contain C but not $(1, \epsilon)$ hence $C_+ = Rad(C)_+$, and by Theorem 5.3 (ii) $C_+ = \mathbb{E}(\mathbb{V}(C))$. We conclude that the intersection of the geometric congruences over C and $Rad(C)$ are the same. □

Remark 7.3.3. It depends whether the $Hom(\mathbb{T}[\boldsymbol{x}]/C, \mathbb{T})$ is taken in the category of idempotent semirings ($\mathbb{B}$-algebras) or $\mathbb{T}$-algebras, in particular whether $\mathbb{T}$ is preserved by these morphisms. If it were the latter, then in the case $n = 1$ the maps $\mathbb{T}[x] \to \mathbb{T}$ are simply evaluation maps and in particular surjective. Note, however, that in the case $n \geq 2$ there are no surjective morphisms $\phi : \mathbb{T}[\boldsymbol{x}] \to \mathbb{T}_n$, which is shown in the following proposition.

Proposition 7.3.4. *There is no surjective morphisms $\phi : \mathbb{T}[x_1, \ldots, x_k] \to \mathbb{T}_n$, for $n > 1$.*

Proof. Assume there is a surjective map $\phi : \mathbb{T}[x_1, \ldots, x_k] \to \mathbb{T}_n$. Notice that for the map ϕ to be surjective we need $k + 1 > n$. Now we have that $\mathbb{T}[x_1, \ldots, x_k]/\ker\phi \cong \mathbb{T}_n$ where $\ker\phi$ is a prime congruence since $\mathbb{T}_n$ is a domain. The multiplicative semigroup of $\mathbb{T}[x_1, \ldots, x_k]/\ker\phi$ is a quotient of $\mathbb{R} \oplus \mathbb{N}^k$ while the multiplicative group of $\mathbb{T}_n$ is $\mathbb{R}^n$. However, $\mathbb{R}^n$ is not a quotient of $\mathbb{R} \oplus \mathbb{N}^k$ unless $n = 1$, which is a contradiction to the choice of n.

□

Note that if the maps ϕ are not surjective then the kernel no longer determines them completely. Consider the following example,

Example 7.3.5. There are infinitely many copies of $\mathbb{Z}_{max}$ embedded into $\mathbb{T}$. Consider the surjective morphism $\mathbb{T}[x] \to \mathbb{Z}_{max}$. Then its kernel is determined by the kernel of the morphism $\mathbb{T}[x] \to \mathbb{T}$, obtained after composing $\mathbb{T}[x] \to \mathbb{Z}_{max}$ with the embedding of $\mathbb{Z}_{max}$ into $\mathbb{T}$. However, if we consider just the maps into $\mathbb{T}$ then the kernel no longer carries the information which copy of $\mathbb{Z}_{max}$ we map onto.

Remark 7.3.6. Analogously to classical algebraic geometry, the $\mathbb{T}$-rational points $Hom_{\mathbb{T}-alg}(\mathbb{T}[\boldsymbol{x}]/C, \mathbb{T})$ is the set of evaluation maps, which are in particular surjective and thus determined by their kernel. The kernels of these maps are the geometric primes containing C.

Lemma 7.3.7. *Every morphism $\phi : \mathbb{T} \to \mathbb{T}$ is of the form $\phi(t^a) = t^{ac}$ for some fixed $c \geq 0$. Furthermore, ϕ is surjective when $c > 0$. In other words a morphism $\mathbb{T} \to \mathbb{T}$ is uniquely determined by the image of t.*

Proof. Let $\phi(t) = t^c$. We want to show that $\phi(t^a) = t^{ac}$. In the case when $a \in \mathbb{Z}$ the statement holds, since ϕ is a morphism. It also holds if $a \in \mathbb{Q}$. If $a \in \mathbb{R} \setminus \mathbb{Q}$, we would like to show that $t^b \in \mathbb{T}$ is the preimage of $t^{b/a}$, or equivalently that $\phi(t^c) = t^{ac}$, for all $c \in \mathbb{R}$. Let $q \in \mathbb{Q}$ and $q > c$, then $t^c + t^q = t^q$ thus $\phi(t^c) + \phi(t^q) = \phi(t^q) = t^{qa}$, so we conclude that $\phi(t^c) < t^{qa}$. Now take $r \in \mathbb{Q}$ and $r < c$, to we conclude that $\phi(t^c) > t^{ra}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$ we get that $\phi(t^c) = t^{ac}$. □

Proposition 7.3.8. *If $\dim(\mathbb{T}[x_1, \ldots, x_k]/P) > 1$, then there is no semiring homomorphism $\phi : \mathbb{T}[x_1, \ldots, x_k] \to \mathbb{T}$, such that $\ker \phi = P$.*

Proof. Let us assume that there exists a semiring homomorphism $\phi : \mathbb{T}[x_1, \ldots, x_k] \to \mathbb{T}$. There are two possibilities. In the first case $\phi(t) = t^a$, for $a > 0$. Note that a cannot be negative, because we define $t > 1$. Then we can see that this map is surjective, for every $t^b \in \mathbb{T}$ is the preimage of $t^{b/a}$. This holds since every automorphism of the additive group of $\mathbb{R}$ that preserves the ordering is linear. Alternatively this follows from Lemma 7.3.7. Hence $\mathbb{T}[x_1, \ldots, x_k]/P \simeq \operatorname{Im} \phi = \mathbb{T}$. But $\dim \mathbb{T} = 1$, hence $\dim(\mathbb{T}[x_1, \ldots, x_k]/P) = 1$ which contradicts the assumption.
In the second case, $\phi(t) = t^0 = 1$ and $\phi(x_i) = t^{a_i}$. Here we can explicitly see that $\ker \phi = P[U]$, where $U = [0 \; a_1 \; \ldots a_n]$. But then $\dim(\mathbb{T}[x_1, \ldots, x_k]/P[U]) = r(U) = 1$ which is a contradiction.

□

Remark 7.3.9. Finitely generated additively idempotent semirings are quotients of a polynomial semiring over $\mathbb{B}$, which has countable cardinality.

Proposition 7.3.10. *Let P be a prime in the polynomial semiring $\mathbb{T}[x_1, \dots, x_k]$, such that $P = P[U]$, for a t-admissible $n \times (k+1)$ matrix U, with $n < k+1$. Then exists a map $\phi : \mathbb{T}[x_1, \dots, x_k] \to \mathbb{T}_n$, such that $P = \ker \phi$.*

Proof. Let U be the matrix, whose i-th row is given by $[\tau_i \ u_{i_1} \ \dots \ u_{i_k}]$, for all $1 \leq i \leq n$. Denote the generator of the l-th copy of $\mathbb{T}$ of $\mathbb{T}_n$ by t_l. Then define the map ϕ,

$$\phi(t) = ({t_1}^{\tau_1}, \dots, {t_n}^{\tau_n})$$

$$\phi(x_j) = ({t_1}^{u_{j_1}}, \dots, {t_n}^{u_{j_n}}),$$

for all $1 \leq j \leq n$.

Note that for two monomials $m_1 = \boldsymbol{x}^{\boldsymbol{a}_1}$ and $m_2 = \boldsymbol{x}^{\boldsymbol{a}_2}$ we have that $(m_1, m_2) \in P$ if and only if $U\boldsymbol{a}_1 = U\boldsymbol{a}_2$ which happens if and only if $\phi(m_1) = \phi(m_2)$. □

Relation to existing tropicalization constructions

The explicit description of prime congruences allows one to interpret the points of the set theoretic tropicalization as geometric congruences of $\mathbb{T}[\boldsymbol{x}]$.

We can also think of the set theoretic tropicalization of a variety X as the $\mathbb{T}$-points of the scheme $\mathcal{T}rop(X)$ as constructed in [GG13]. If $X = Spec\ A$, where A is a k-algebra and k is a valued field, then the set of these points can be obtained as the image of the Berkovich analytification of X under the standard tropicalization map. The Berkovich analytification of X is the set of rank one valuations on A compatible with k.

On the other hand, the $\mathbb{T}_n$-points of $\mathcal{T}rop(X)$ correspond to the points of the Hahn tropicalization [FR15], which is a tropicalization over a higher rank valued field (higher rank setting was initially studied by [Ba12]). The $\mathbb{T}_n$-points of the universal embedding constructed in [GG14] are the same as the points of the Hahn analytification. One of my ongoing research projects focuses on investigating the relation between the primes of higher rank (corresponding to a matrix of rank greater than 1) and the points on the Hahn analytification.

Bibliography

[AA94] F. Alarcón and D. Anderson, *Commutative semirings and their lattices of ideals*, Houston Journal of Mathematics, Volume 20, No. 4, 1994

[Ba12] S. Banerjee, *Tropical geometry over higher dimensional local fields.*, arXiv:1105.5873

[Ber11] V. Berkovich, *Analytic geometry over F1.* Slides, 2011. Online available http://www.wisdom.weizmann.ac.il/ vova/Padova-slides 2011.pdf.

[BE13] A. Bertram and R. Easton, *The Tropical Nullstellensatz for Congruences*, preprint, http://www.robertweaston.com/wp-content/uploads/documents/papers/Tropical_Null.pdf

[CC13] A. Connes and C. Consani, *Projective geometry in characteristic one and the epicyclic category*, Nagoya Mathematical Journal 217 (2015), 95-132.

[CC14] A. Connes and C. Consani, *The Arithmetic Site*, to appear in Comptes Rendus Mathematique, arXiv:1405.4527

[CC15] A. Connes and C. Consani, *The Scaling Site*, arXiv:1507.05818

[CDPR12] F. Cools, J. Draisma, S. Payne and E. Robeva, *A tropical proof of the Brill-Noether theorem*, Adv. Math. 230 (2012), no. 2, 759-776.

[Dei05] A. Deitmar *Schemes over* $\mathbb{F}_1$. Number fields and function fieldstwo parallel worlds, Progr. Math., vol. 239, 2005.

[Dei08] A. Deitmar, $\mathbb{F}_1$ *schemes and toric varieties.* Contributions to Algebra and Geometry Vol. 49, No. 2 (2008), pp. 517-525.

[Ei95] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Graduate Texts in Mathematics, 1995, Springer-Verlag, volume 150.

[FR15] T. Foster and D. Ranganathan, *Hahn analytification and connectivity of higher rank tropical varieties*, arXiv:1504.07207

[IR14] Z. Izhakian and L. Rowen, *Congruences and coordinate semirings of tropical varieties*, arXiv: 1408.2428

[GG13] J. Giansiracusa and N. Giansiracusa, *Equations of tropical varieties*, arXiv:1308.0042

[GG14] J. Giansiracusa and N. Giansiracusa, *The universal tropicalization and the Berkovich analytification*, arXiv:1410.4348

[Go99] J. Golan, *Semirings and Their Applications*, Kluwer, Dordrecht, 1999

[GP14] D. Grigoriev and V. Podolskii, *Tropical Effective Primary and Dual Nullstellensätze*, arXiv:1409.6215v1.

[Gro10] M. Gross, *Mirror symmetry for $\mathbb{P}^2$ and tropical geometry*, Adv. Math. 224 (2010), no. 1, 169245.

[Gro11] M. Gross, *Tropical geometry and mirror symmetry*, CBMS Regional Conference Series in Mathematics, vol. 114, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2011.

[JP15] D. Jensen and S. Payne, *Tropical independence II: The maximal rank conjecture for quadrics* arXiv:1505.05460

[JM14] D. Joó and K. Mincheva, *Prime congruences of idempotent semirings and a Nullstellensatz for tropical polynomials*, arXiv:1408.3817

[Les12] P. Lescot, *Absolute Algebra III-The saturated spectrum*, Journal of Pure and Applied Algebra 216 (2012), no. 7, 1004-1015.

[Lor12] O. Lorscheid, *The geometry of blueprints: Part I: Algebraic background and scheme theory*, Adv. Math. 229 (2012), no. 3, 1804-1846.

[MR14] D. Maclagan and F. Rincón, *Tropical schemes, tropical cycles, and valuated matroids*, arXiv:1401.4654

[MS] D. Maclagan and B. Sturmfels, *Introduction to tropical geometry* Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, vol. 161, 2015

[Man11] C. Manon, *Dissimilarity maps on trees and the representation theory of $SL_m(\mathbb{C})$*, J. Algebraic Combin. 33 (2011), no. 2, 199213.

[Mik05] G. Mikhalkin, *Enumerative tropical algebraic geometry in $\mathbb{R}^2$*, J. Amer. Math. Soc. 18 (2005), no. 2, 313377.

[Mik06] G. Mikhalkin, *Tropical geometry and its applications*, International Congress of Mathematicians. Vol. II, Eur. Math. Soc., Zürich, 2006, 827-852. MR 2275625 (2008c:14077)

[PS04] L. Pachter and B. Sturmfels, *Tropical geometry of statistical models*, Proc. Natl. Acad. Sci. USA 101 (2004), no. 46, 1613216137 (electronic).

[PR14] T. Perri and L. Rowen, *A tropical Krull-Schmidt theorem* , arXiv:1408.4757

[PR15] T. Perri and L. Rowen, *Kernels in tropical geometry and a Jordan-Hlder Theorem*, arXiv:1405.0115

[RSS13] Q. Ren, S. Sam and Bernd Sturmfels, *Tropicalization of classical moduli spaces*, arXiv:1303.1132, 2013.

[Rob85] L. Robbiano, *Term orderings on the polynomial ring*, EUROCAL 85, Vol. 2 (Linz, 1985), Lecture Notes in Comput. Sci. 204, 513-517, Springer, Berlin (1985)

[Se54] A. Seidenberg, *On the dimension theory of rings II*, Pacific J. Math. 4 (1954) 603-614.

[Tev07] J. Tevelev, *Compactifications of subvarieties of tori*, Amer. J. Math. 129 (2007), no. 4, 10871104.

[Tit56] J. Tits, *Sur les analogues algébriques des groupes semi-simples complexes*, Colloque d'algèbre supérieure, tenu à Bruxelles du 19 au 22 décembre 1956, Centre Belge de Recherches Mathématiques Établissements Ceuterick, Louvain; Librairie Gauthier-Villars, Paris (1957), 261-289.

Curriculum Vitae

Kalina Mincheva was born on December 28, 1985 in Bulgaria. In 2008, she received BA degrees in Mathematics and Computer Science from the American University in Bulgaria (AUBG). In 2010 she obtained a MSc degree in Mathematics from the Central European University (CEU) in Budapest, Hungary, under the supervision of Professor Pál Hegedűs. The topic of the thesis was "Automorphisms of non-abelian p-groups". Her PhD dissertation was completed under the guidance of Professor Caterina Consani and Professor Jack Morava and was defended on March 1, 2016.