FAKULTÄT FÜR MATHEMATIK, INFORMATIK
UND NATURWISSENSCHAFTEN

RHEINISCH-WESTFÄLISCHE TECHNISCHE
HOCHSCHULE AACHEN

Masterarbeit in Mathematik

im Februar 2014

Geometric Aspects of Mixed Difference Ideals

Andrés W. Goens Jokisch

LEHRSTUHL FÜR MATHEMATIK (ALGEBRA)

Prof. Dr. Julia Hartmann

Acknowledgments

I would like to thank Michael Wibmer, for his patience, ideas and support throughout the work on this thesis. Writing this thesis would certainly not have been possible if it was not for his mentoring. In the time spent working on this thesis, I did not only learn about difference algebra, but also how to do mathematics in general, and I have Michael Wibmer to thank for this. I would also like to thank Julia Hartmann for her patience and help in writing this thesis. Finally, I would like to thank Daniel Rettstadt, Annette Maier and Stefan Ernst for always offering advice the numerous times I had smaller and not-so-small problems and/or questions.

Contents

Introduction

In a field k, the polynomial y^n has only a single solution for any n, namely 0. There is obviously a difference, however, between the equations $y = 0$ and $y^2 = 0$ for example. In particular, the solution 0 has a different 'multiplicity' for different exponents n. We cannot establish this difference by simply looking at the solutions of these polynomials over a field. A way we can distinguish y and y^2 is by looking for solutions elsewhere, not only in fields. Over a general k-algebra, for example, the sets of solutions of the equations $y = 0$ and $y^2 = 0$ could be different.

On a related note, the ideals generated by the two polynomials, (y) and $(y^2) \trianglelefteq k[y]$ are different. However, the radicals of these ideals are equal,

$$\sqrt{(y)} = (y) = \sqrt{(y^2)},$$

which means we cannot distinguish the polynomials like that either. Instead of considering the coordinate rings of the varieties, we could capture this 'multiplicity' by studying the ring $k[y]/(y^n)$. The k-dimension of this ring is n, which is exactly what we would like to define as the multiplicity.

A similar problem arises in difference algebra, where we consider rings (fields) equipped with an endomorphism which we usually denote by σ and call a *difference operator*. We call the tuple of the ring (field) and the endomorphism a *difference ring (field)*. The analogous concept to polynomial rings is that of so-called *difference polynomial rings*. We consider difference polynomial rings as polynomial rings on infinitely many variables, a subset of which we call *difference variables* and the others represent the powers of σ applied to a difference variable. For example, the difference polynomial ring in the difference variable y is the polynomial ring in the infinitely many variables $y, \sigma(y), \sigma^2(y), \ldots$. The variables $y, \sigma(y), \sigma^2(y), \ldots$ are algebraically independent. Here, instead of the degree of the polynomial, we are interested in the *order* of the difference equation. In analogy to the equation $y^n = 0$, we can consider the difference equation $\sigma^n(y) = 0$. This is a difference equation of order n. However, in a difference field k there is only one solution to the equation $\sigma^n(y) = 0$: Since σ is an endomorphism of the field k, it has to be injective. Thus, $\sigma^n(y) = 0$ implies that $y = 0$.

We would like to study difference equations and their solutions in such a way that we can distinguish between $\sigma(y) = 0$ and $\sigma^2(y) = 0$. Just as in the analogy for the polynomials y and y^2, there seems to be a sort of 'multiplicity' of the solution 0 in the difference equation $\sigma^2(y) = 0$. We would also like

to have a way of finding this 'multiplicity' of the solutions we just described.

In this thesis, we adapt the standard concepts used in difference algebra to deal with this. As suggested by the analogy above, we achieve this by changing the type of structure where we look for solutions of the difference equations. Instead of looking for solutions in difference fields, we consider difference rings which are integral domains. The endomorphism σ does not have to be injective anymore, and thus, the two difference equations $\sigma^2(y) = 0$ and $\sigma(y) = 0$ can have different sets of solutions.

When studying difference equations one is interested in so-called *difference ideals*, which are the ideals that are stable under σ. As in algebraic geometry, to a set of difference equations F we will associate an analog to algebraic sets, which shall be denoted by $\mathbb{V}_m(F)$, and call it *mixed difference variety*. This object can be interpreted as the set of solutions to the system of difference equations F and takes the additional solutions discussed above into account. Mixed difference varieties are analogous to, but different from the difference varieties usually studied in difference algebra. We also introduce concepts analogous to the concepts of vanishing ideals and the Zariski topology. A further analogy we obtain are the concepts of σ-degree and σ-dimension, both of which are related to the concept of the Krull dimension. The σ-degree gives a precise way to quantify the 'multiplicity' of the solutions of a system of difference equations. This new approach to solutions of difference equations through mixed difference varieties will be seen to be closely related to a class of difference ideals called *mixed difference ideals*, similar to the way affine algebraic varieties are related to radical ideals. The following theorem is one of the main results of this thesis. It is a far-reaching generalization of the simple statement that the equation $\sigma^n(y) = 0$ has a solution of 'multiplicity' n.

Theorem (4.22)**.** *Let k be a difference field and let $f \notin k$ be an irreducible difference polynomial in n difference variables. Then $\mathbb{V}_m(f)$ has an irreducible closed subset X such that the σ-dimension of X is $n-1$ and the σ-degree of X equals the order of f.*

To prove the theorem above, we consider so-called *difference kernels*. In a difference polynomial ring, even if we only have one '*difference variable*' we have an infinite number of algebraically independent variables when considered as a polynomial ring. Such rings are not Noetherian, and thus, some difficulties arise when attempting to study them.

The idea behind difference kernels is the following. In order to study a difference ideal $\mathfrak{a}$ in a difference polynomial ring $k[y, \sigma(y), \sigma^2(y), \ldots]$, we

study the intersection of the ideal with the polynomial ring generated by a finite number of variables, and call it a *difference kernel*:

$$\mathfrak{a}[d] := \mathfrak{a} \cap k[y, \sigma(y), \ldots, \sigma^d(y)].$$

We can then study how the properties that $\mathfrak{a}[d]$ has depend on the properties of the difference ideal $\mathfrak{a}$. At least as interesting is the question how it works the other way around. What properties of an ideal $I \trianglelefteq k[y, \sigma(y), \ldots, \sigma^d(y)]$ ensure that there exists a so-called *realization* of this ideal, that is, a difference ideal $\mathfrak{a}$ in the difference polynomial ring such that $I = \mathfrak{a}[d]$? If that is the case, how do the properties of I affect those of $\mathfrak{a}$? For a class of difference ideals called *σ-prime difference ideals* the answers to the former questions are known. There is a characterization of the ideals $I \trianglelefteq k[y, \sigma(y), \ldots, \sigma^d(y)]$ for which there exists a realization as a σ-prime difference ideal. For the concepts developed in this thesis, however, a larger class of difference ideals is interesting. We are interested in difference ideals that are prime.

Unfortunately, a full characterization of the ideals of $k[y, \ldots, \sigma^d(y)]$ for which there exists a realization that is a prime difference ideal was not found. However, some results in this direction were achieved. Another main result of this thesis is a characterization of the prime difference kernels that can be extended from $k[y, \ldots, \sigma^d(y)]$ to $k[y, \ldots, \sigma^{d+1}(y)]$. A conjecture is given of a possible characterization of the ideals of $k[y, \ldots, \sigma^d(y)]$ which have a realization as a prime difference ideal.

This thesis is divided into four sections. Section 1 will introduce the subject of difference algebra, present the most basic definitions and some of the well-known results concerning the standard theory of perfect difference ideals and their geometric aspects. The rest of the thesis will then deal with the generalizations of the material in Section 1 to the case of mixed difference ideals. Section 2 begins with a more in-depth study of difference ideals, with a particular emphasis on mixed difference ideals. It also touches on some geometrical subjects, defining a topological space similar to the Zariski topology on a special class of ideals of a difference ring. Section 3 continues with a more geometric nature, presenting a definition of mixed difference varieties as well as some basic properties of these. Finally, Section 4 deals with difference kernels. The two main results and the conjecture stated above are presented here.

Conventions on Notation for this Thesis

We will use the following conventions throughout the thesis:

- $\mathbb{N} := \{0, 1, \ldots\}$
- $\mathbb{N}_{\geq 1} := \{1, 2, \ldots\}$
- $\underline{n} := \{1, 2, \ldots, n\}$
- $\underline{n}_0 := n \cup \{0\}$
- $A \setminus B = \{a \in A \mid a \notin B\}$
- Rings will be assumed to be commutative and unital.
- Let R be a ring, $a_1, \ldots, a_n \in R$. Then $(a_1, \ldots, a_n)$ denotes the smallest ideal of R containing $a_1, \ldots, a_n$.
- Let R be a difference ring, $a_1, \ldots, a_n \in R$. Then $[a_1, \ldots, a_n]$ denotes the smallest difference ideal of R containing $a_1, \ldots, a_n$.
- Let R be a difference ring. Then $A \trianglelefteq_\sigma R$ means that A is a difference ideal of R.
- The variable y in (difference) polynomial rings will, in general, mean n variables $y_1, \ldots, y_n$, i.e., we will write for example $k[y]$ for $k[y_1, \ldots, y_n]$.

1 Difference Algebra

In this chapter, we will introduce the basic notions of difference algebra. These basic concepts and definitions are indispensable for the rest of this thesis. The aim of this chapter is to supply all the information necessary for the reader who has no knowledge of difference algebra, but is familiar with algebra and algebraic geometry. The two standard textbooks in the field that proved most useful for this thesis are the works of Cohn [5] and Levin [6]. A reader who has interest in a more thorough treatment of the subject should look into any of the two. While the book by Cohn is perhaps more accessible and easier to read, it has a notation that might be considered cumbersome by some modern standards. The textbook by Levin considers a more general setting by working with partial difference equations that are not treated in this thesis. Additionally, a reader might find M.Wibmer's lecture notes on difference algebra [1] useful for reading this thesis, since they resemble this thesis in the way the subjects are structured.

1.1 Introduction to Difference Algebra

Difference algebra is branch of mathematics whose origin is closely related to that of differential algebra. We will only introduce the object of study here. A detailed historical review of the origin of difference algebra can be found in the preface of [6].

To offer a first idea of the objects of study of difference algebra, we will start off with some examples of difference equations. Probably one of the best known examples comes from the Fibonacci sequence: $1, 1, 2, 3, 5, 8, 13, \ldots$, which can be seen as a solution of the following recursive equation:

$$a_0 = 1, a_1 = 1,$$
$$a_n = a_{n-1} + a_{n-2}, n \geq 2.$$

Another example that any mathematician or physicist will know is the functional equation of the Γ-function:

$$\Gamma(x+1) = x\Gamma(x).$$

A classical result in complex analysis states that any function which satisfies this equation is a multiple of the Γ-function, which is considered a generalization of the factorial. An integral representation of the Γ-function is given by

$$\Gamma(x) = \int_0^\infty \frac{t^x}{t} e^{-t} dt.$$

These are two notable examples of difference equations, as we will soon see. In difference algebra, however, we do not seek to find 'explicit' solutions of these equations, as are the numbers in the Fibonacci sequence or the integral representation of the Γ-function. Rather, we seek to study the structure of these equations and tackle problems, such as the existence of solutions, in a more abstract sense.

1.2 Basics of Difference Algebra

Definition 1.1. *Let R be a ring (in this thesis all rings will be commutative and unital), and let $\sigma : R \to R$ be an endomorphism of rings in R. Then we call the tuple (R, σ) a* difference ring*, or* σ-ring*.*

By abuse of notation we will say that R is a σ-ring to refer to the pair, and if R' is a further σ-ring, we will also use the symbol σ for the endomorphism on R'. This should not lead to confusion, since it can be inferred from the context which of the endomorphisms is meant.

Definition 1.2. *Let R, R' be σ-rings and let $\varphi : R \to R'$ be a morphism of rings. We say that φ is a* morphism of σ-rings *if*

$$\sigma(\varphi(r)) = \varphi(\sigma(r)) \text{ for all } r \in R.$$

Example 1.3. *A few of the more notable examples of σ-rings are the following:*

- *Every ring R is a σ-ring with $\sigma = Id_R$. We call this a* constant σ-ring*.*

- *The field of meromorphic functions $\mathbb{C} \to \mathbb{C}$, which we will denote by $\mathcal{M}$, is a σ-ring with $\sigma(f)(x) = f(x+1)$ for every $x \in \mathbb{C}$, $f \in \mathcal{M}$. Similarly, for $q \in \mathbb{C}$, $|q| = 1$, the mapping $\sigma(f)(x) := f(qx)$ also defines a σ-ring structure on $\mathcal{M}$.*

- *The sequences of integers, which we will denote by $Seq(\mathbb{Z})$, are a σ-ring with the operation of shifting its terms to the left:*

$$\sigma : (a_n)_{n\in\mathbb{N}} \mapsto (a_{n+1})_{n\in\mathbb{N}}.$$

Definition 1.4. *Let R be a σ-ring. If R is also a field, we call the pair (R, σ) a* σ-field*. If k is a σ-field, A a σ-ring, and we have a morphism of rings $\varphi\colon k \to A$ such that $\varphi\sigma = \sigma\varphi$ then we call A a* k-σ-algebra*. In this case we can also consider A as a k-algebra via φ.*

Example 1.5. *Let k be a σ-field. We consider the polynomial ring in infinitely many variables $R := k[y_1, \sigma(y_1), \sigma^2(y_1), \ldots]$, where $y_1, \sigma(y_1), \sigma^2(y_1), \ldots$ are, for the moment at least, simply the names of (algebraically independent) variables. This ring can be turned into a k-σ-algebra by defining:*

$$\sigma : R \to R, y_1 \mapsto \sigma(y_1), \sigma^{n-1}(y_1) \mapsto \sigma^n(y_1) \text{ for all } n > 1$$

and extending this mapping in the obvious way.

Definition 1.6. *The σ-ring defined in Example 1.5 is called a* σ-polynomial ring. *We denote this σ-polynomial ring by $k\{y_1\}$. In an analogous fashion we can define σ-polynomial rings $k\{y_1, \ldots, y_n\} =: k\{y\}$ in many variables. We will use the shorthand notation $y = (y_1, \ldots, y_n)$ throughout this thesis.*

At this point we can express (polynomial) difference equations as difference polynomials. We would like to have a concept of the order of an equation.

Definition 1.7. *Let k be a σ-field and consider the polynomial ring $k\{y\}$ on n difference variables. For a monomial $m = a\sigma^{r_1}(y_1) \cdots \sigma^{r_n}(y_n)$ with $0 \neq a \in k$ we define the* order *of m to be*

$$\mathrm{Ord}(m) = \max_{i=1,\ldots,n} r_i.$$

For a polynomial $f \in k\{y\}$ we define the order *of f, $\mathrm{Ord}(f)$ to be the maximal order of a monomial effectively appearing in f (with a non-zero coefficient in a representation with unique monomials) We define the* effective order *of f, $\mathrm{Eord}(f)$ to be the difference between the maximal and minimal orders of monomials effectively appearing in f.*

Definition 1.8.

- *Given a σ-ring S and a subring $R \leq S$, we say that R is a* σ-subring *of S if $(R, \sigma|_R)$ is a σ-ring, i.e. if the image of $\sigma|_R$ is contained in R.*
- *Let R be a σ-ring. A* σ-ideal *is an ideal $I \trianglelefteq R$ which is closed under σ. This means that $\sigma(I) \subseteq I$. We will use the notation $I \trianglelefteq_\sigma R$ for this. In this case, there exists a canonical σ-ring structure on the quotient ring R/I:*

$$\sigma : R/I \to R/I, a + I \mapsto \sigma(a) + I.$$

A useful way of working with difference ideals is to consider a difference-algebraic concept of generating sets.

Definition 1.9. *Let R be a σ-ring and let $\mathfrak{a} \trianglelefteq_\sigma R$ be a σ-ideal of R. Let $a_j \in R$ for all $j \in J$, where J is an index set. We use $[a_j \mid j \in J]$ to denote the σ-ideal minimal (with respect to inclusion) of R which contains all a_j for $j \in J$. In fact, $[a_j \mid j \in J]$ is equal to the set*

$$\left\{ \sum_{i=1}^{n} b_i \sigma^{r_i}(x_i) \mid n \geq 0, r_i \geq 0, b_i \in R, x_i \in \{a_j, \mid j \in J\}, i = 1, \ldots, n \right\}.$$

If there exist $b_1, \ldots, b_r \in \mathfrak{a}$, such that $\mathfrak{a} = [b_j \mid j \in \{1, \ldots r\}] =: [b_1, \ldots, b_r]$, we say that $\mathfrak{a}$ is finitely σ-generated *as a σ-ideal.*

There are numerous properties in which we are interested for studying difference ideals. For the scope of this thesis, the most important ones are the following:

Definition 1.10. *Let $\mathfrak{a} \trianglelefteq_\sigma R$ be a σ-ideal of R.*

- $\mathfrak{a}$ *is called* perfect*, if $\sigma^{i_1}(f) \cdots \sigma^{i_n}(f) \in \mathfrak{a}$ implies that $f \in \mathfrak{a}$, where $n \in \mathbb{N}_{\geq 1}, i_j \in \mathbb{N}$ for all $j \in \underline{n}$.*
- $\mathfrak{a}$ *is called* reflexive*, if $\sigma(f) \in \mathfrak{a}$ implies $f \in \mathfrak{a}$.*
- $\mathfrak{a}$ *is called* σ-prime*, if $\mathfrak{a}$ is a prime, reflexive σ-ideal.*
- *The ring R is called* perfectly σ-reduced*, if the zero σ-ideal (the intersection of all σ-ideals) is perfect.*

Similar to σ-generators of ideals, we can define generators of a k-σ-algebra.

Definition 1.11. *A k-σ-algebra A is* finitely σ-generated *if there exist elements $f_1, \ldots, f_n$ such that*

$$A = k[f_1, f_2, \ldots, f_n, \sigma(f_1), \ldots, \sigma(f_n), \sigma^2(f_1), \ldots].$$

We write $k\{f_1, \ldots, f_n\}$ to denote the σ-algebra generated by $f_1, \ldots, f_n$.

Remark 1.12. If A is a k-σ-algebra, σ-generated by $f_1, \ldots, f_n$, then we have a canonical epimorphism of k-σ-algebras from the σ-polynomial ring $k\{y_1, \ldots, y_n\}$ to A: $y_i \mapsto f_i, i = 1, \ldots, n$. We thus see that σ-polynomial rings are free objects in the category of finitely generated k-σ-algebras.

Definition 1.13. *If the kernel I of the epimorphism mentioned in Remark 1.12 is finitely σ-generated as well, say, by $r_1, \ldots, r_m$, then we call the algebra A* finitely σ-presented.

Remark 1.14. In the conditions of the previous definition, by the fundamental theorem on homomorphisms we have $A \cong k\{y_1, \ldots, y_n\}/[r_1, \ldots, r_m]$. Note as well that the concepts "finitely σ-generated" and "finitely σ-presented" are truly different, contrary to the case of polynomial rings over fields where we can argue with the Hilbert basis theorem. This difference can be seen in the next example.

Example 1.15. *Let k be a σ-field and let $I \trianglelefteq_\sigma k\{y\}$ be the σ-ideal σ-generated by $y\sigma(y), y\sigma^2(y), y\sigma^3(y), \ldots$, i.e., $I = [y\sigma^i(y) \mid i \geq 1]$. Then the σ-ring $R := k\{y\}/I$ (where $\sigma(r+I) := \sigma(r)+I$) is finitely σ-generated, $R = k\{y+I\}$, but not finitely σ-presented, since I is not finitely σ-generated.*

We can now return to the examples from the beginning of this chapter, as we now have the necessary concepts to formulate these in the language of difference algebra.

Example 1.16. *The Fibonacci sequence is a solution to the σ-polynomial $\sigma^2(y)-\sigma(y)-y$ in the σ-ring $Seq(\mathbb{Z})$. This is precisely the recurrence relation $a_{n+2} = a_{n+1} + a_n$. In the same way, the Γ-function is the solution to the σ-polynomial $\sigma(y) - zy$, where $z \in \mathbb{C}(z)$ denotes the identity function $z \mapsto z$ in the σ-ring $\mathcal{M} \supset \mathbb{C}(z)$.*

1.3 Perfect Difference Ideals And Difference Varieties

The purpose of this section is to present in a compact fashion some well-known results of difference algebra, mainly about the geometric aspects of perfect difference ideals. The rest of this thesis will then try to generalize many of these results to the case of mixed ideals. For the sake of compactness, the results shall be stated without proof. Similarly, many of the examples and remarks that offer a more in-depth understanding of said results will be deferred to the later sections of the thesis. These will be presented alongside the corresponding generalizations of the results.

Definition 1.17. *Let R be a σ-ring and $F \subset R$ be a subset of R. The smallest (with respect to inclusion) perfect σ-ideal containing F is called the* perfect closure of F *and we will write $\{F\}$ to denote it.*

Perfect difference ideals will play a role similar to that of radical ideals in algebraic geometry. In fact, in the case of a constant σ-ring the definition of perfect difference ideals corresponds to that of radical ideals. Most of the following results can easily be recognized as generalizations of standard results in algebraic geometry.

Theorem 1.18. *Let R be a σ-ring and $F \subseteq R$ be a subset of R. Then we can write the perfect closure of F as follows:*

$$\{F\} = \bigcap_{\substack{F \subseteq \mathfrak{p} \trianglelefteq_\sigma R, \\ \mathfrak{p} \ \sigma\text{-prime}}} \mathfrak{p}. \tag{1}$$

Proof. See Proposition 2.3.4 of [6] □

If a difference ring R satisfies the ascending chain condition for perfect difference ideals, we say that R is a *Ritt difference ring*. A much stronger version of the previous fact can actually be proven for this particular class of difference Rings. Consider a Ritt difference Ring R and a perfect difference ideal $\mathfrak{a} \trianglelefteq_\sigma R$. For a decomposition of $\mathfrak{a}$ as in Equation 1, let

$$\mathfrak{a} = \{\mathfrak{a}\} = \bigcap_{i \in I} \mathfrak{p}_i,$$

where I is an index set and $\mathfrak{p}_i$ a σ-prime difference ideal of R for all $i \in I$. For a subset $J \subseteq I$, such that

$$\mathfrak{a} = \bigcap_{i \in J} \mathfrak{p}_i,$$

we say that J is an *irredundant decomposition of* $\mathfrak{a}$, if $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for all $i \neq j$.

It can be shown that in a Ritt difference ring there is a unique finite irredundant decomposition in σ-prime ideals for every perfect difference ideal. See, for example, Theorem 2.5.7 of [6].

Ritt difference rings are of particular interest as, in a way, they fulfill some of the roles played by Noetherian rings in the standard results of algebraic geometry/commutative algebra. In particular, a result analogous to the Hilbert basis theorem can be proven for Ritt difference rings:

Theorem 1.19. *Let R be a Ritt difference ring and consider the difference polynomial ring $R\{y_1, \ldots, y_n\}$ in n difference variables. Then $R\{y_1, \ldots, y_n\}$ is a Ritt difference ring as well.*

Proof. See Theorem 2.5.11 of [6] □

A further important analogy of a more geometric nature can be made by generalizing the Zariski topology on the spectrum of a ring. We call the set of all σ-prime ideals of a difference ring R the *σ-spectrum* or *difference spectrum* of R, and use the symbol $\mathrm{Spec}^\sigma(R)$ for it.

Definition 1.20. *Let R be a difference ring, $F \subseteq R$ a subset. We set $\mathcal{V}(F) := \{\mathfrak{p} \in \mathrm{Spec}^\sigma(R) \mid F \subseteq \mathfrak{p}\}$.*

It can be shown that we can define a topology in $\mathrm{Spec}^\sigma(R)$ by letting a set be closed if and only if it is of the form $\mathcal{V}(F)$ for $F \subseteq R$. In fact, this topology is just the restriction of the usual Zariski topology on $\mathrm{Spec}(R)$ to $\mathrm{Spec}^\sigma(R)$. We call this topology on $\mathrm{Spec}^\sigma(R)$ the *Cohn topology*. A few interesting properties of the Cohn topology on $\mathrm{Spec}^\sigma(R)$ are presented in the following Proposition:

Proposition 1.21. *Let R be a difference ring. Then:*

- *The mapping*

$$\{\mathfrak{a} \trianglelefteq_\sigma R \mid \mathfrak{a} \text{ perfect } \} \to \{A \subseteq \mathrm{Spec}^\sigma(R) \mid A \text{ closed } \}, \mathfrak{a} \mapsto \mathcal{V}(\mathfrak{a})$$

  is bijective and order-reversing.

- *For $F \subseteq R$, $\mathcal{V}(F)$ is irreducible, if and only if $\{F\}$ is prime.*

- $\mathrm{Spec}^\sigma(R)$ *is a quasi-compact topological space. It is Noetherian, if and only if R is Ritt.*

Proof. See Propositions 1.2.35 and 3.3.4 of [1] □

In what follows we continue to explore the more geometric aspects of the basic theory of perfect difference ideals. For this, we will address the analogous concept to affine varieties next. To define these, we will first introduce the following notation: Let k be a σ-field and $k\{y_1, \ldots, y_n\}$ a difference polynomial ring in n variables. Further let $K \supseteq k$ be a σ-field extension of k and $F \subseteq k\{y_1, \ldots, y_n\}$. Then we set

$$\mathbb{V}_K(F) := \{x \in K^n \mid f(x) = 0 \text{ for all } f \in F\}.$$

With this notation we can define (affine) difference varieties.

Definition 1.22. *Let k be a σ-field. A functor X from the category of σ-field extensions of k to the category of sets is called* σ-variety *or* difference variety *if there exists a subset $F \subseteq k\{y_1, \ldots, y_n\}$ of a σ-polynomial ring over k such that $X(K) = \mathbb{V}_K(F)$ for all σ-field extensions K of k.*

Since we will only study this concept of difference variety, we will not explicitly refer to them as affine.

To establish a connection between difference varieties and perfect difference ideals we will introduce a further symbol, which bears much resemblance

to the standard definition in algebraic geometry. For a difference variety $X = \mathbb{V}(F), F \subseteq k\{y_1, \ldots, y_n\}$ we set

$$\mathbb{I}(X) := \{f \in k\{y_1, \ldots, y_n\} \mid f(a) = 0 \text{ for all } a \in \mathbb{V}_K(F) \\ \text{for all } K \supseteq k \text{ } \sigma\text{-field extension}\}.$$

With these concepts and definitions, the analogy can further unfold. As stated before, it can be shown that - in a way - perfect difference ideals are a difference-algebraic generalization of radical ideals. The following result serves to expand on this idea.

Proposition 1.23. *Let k be a σ-field and $F \subseteq k\{y_1, \ldots, y_n\}$. Then*

$$\mathbb{I}(\mathbb{V}(F)) = \{F\}$$

Proof. See Proposition 2.1.11 of [1] □

A very useful tool in algebraic geometry for studying affine varieties are coordinate rings. The same principle can be applied for difference varieties. Let $X = \mathbb{V}(F), F \subseteq k\{y_1, \ldots, y_n\}$ be a difference variety. Then we can associate a *difference coordinate ring* to X by defining

$$k\{X\} := k\{y_1, \ldots, y_n\}/\mathbb{I}(X).$$

It can be shown, for example, that the perfect σ-ideals of the coordinate ring of a difference variety X are in inclusion-reversing bijection to the σ-subvarieties of X. We exclude a formal definition of σ-subvarieties at this point, as it will be treated in the case of mixed ideals later, and as the details are basically the same.

Another noteworthy bijection deals with solutions of difference equations. Let k be a σ-field and $K, L \supseteq k$ be σ-field extensions of k. Further, let $F \subseteq k\{y_1, \ldots, y_n\}$ be a system of difference equations. We say that two solutions of F, $a \in K, a' \in L$ (this means that $f(a) = 0 = f(a')$ for all $f \in F$) are *equivalent* if the mapping

$$k\langle a \rangle \to k\langle a' \rangle, a \mapsto a'$$

is an isomorphism of σ-fields. Here, $k\langle a \rangle \subseteq K$ denotes the smallest (with respect to inclusion) σ-subfield of K containing a and k, and similarly for a' and L.

Proposition 1.24. *Let k be a σ-field and $X = \mathbb{V}(F)$ a difference variety over k. Then the equivalence classes of solutions of F are in bijection to the σ-spectrum of the coordinate ring,* $\mathrm{Spec}^\sigma(k\{X\})$.

Proof. See Theorem 2.2.1 of [1] □

The relationship between σ-varieties over a σ-field k and their coordinate ring can be identified with a category-theoretical result. It can be shown that for a σ-field k, the category of σ-varieties over k is anti-equivalent to the cateogry of k-σ-algebras which are perfectly σ-reduced and finitely σ-generated.

To conclude this brief survey of some of the standard geometric aspects of difference algebra, we will present a final interesting result. There are concepts of *σ-degree*, σ-deg and *σ-dimension*, σ-dim, that can be associated with a difference variety. They will be formally defined later on.

Theorem 1.25. *Let k be a σ-field and $f \in k\{y_1, \ldots, y_n\}$, $f \notin k$ an irreducible σ-polynomial such that* $\mathrm{Eord}(f) = \mathrm{Ord}(f)$. *Then $\mathbb{V}(f) \subset \mathbb{A}_k^n$ has an irreducible component X such that* $\sigma\text{-dim}(X) = n - 1$ *and* $\sigma\text{-deg}(X) = \mathrm{Ord}(f)$.

Proof. See Theorem 5.2.14 of [1]. □

2 Difference Ideals

In this section we study difference ideals more closely. A special focus will be put on mixed and prime difference ideals, which in many ways mimic the properties of and relationship between radical and prime ideals on commutative rings. Much of the following is based on Section 1.2 of the lecture notes of M. Wibmer [1], where most of this has been worked out for the analogous case of perfect and σ-prime difference ideals.

2.1 Difference Ideals

We recall Definition 1.10, and consider an additional type of difference ideal here.

Definition 2.1. *Let $\mathfrak{a} \trianglelefteq_\sigma R$ be a σ-ideal of R.*

- *Then $\mathfrak{a}$ is called a* mixed σ-ideal *if for any $f, g \in R$ with $fg \in \mathfrak{a}$ it follows that $f\sigma(g) \in \mathfrak{a}$.*
- *The ring R is called* well-mixed*, if the zero ideal $[0]$ is mixed.*

Remark 2.2. It is easy to see from the definitions that σ-prime σ-ideals are perfect, and that perfect σ-ideals are mixed, radical and reflexive. Prime σ-ideals are also mixed, but not necessarily perfect. Note that there is a difference between a prime σ-ideal and a σ-prime σ-ideal: the former does not necessarily have to be reflexive, while the latter does. Both, prime σ-ideals and σ-prime ideals will be very important throughout this thesis. It is for this reason that the distinction between both is of utmost importance.

The above properties behave well with respect to morphisms of σ-rings in the sense of the following lemma (see Exercise 1.2.7 of [1]):

Lemma 2.3. *Let $\varphi : R \to S$ be a morphism of σ-rings and $\mathfrak{a} \trianglelefteq_\sigma S$ a σ-ideal of S. Then $\varphi^{-1}(\mathfrak{a}) \trianglelefteq_\sigma R$ is a σ-ideal of R. Similarly, if $\mathfrak{a}$ is a mixed σ-ideal, then so is $\varphi^{-1}(\mathfrak{a})$. The same is true for perfect, prime and for reflexive σ-ideals.*

Proof. Since $\mathfrak{a} \trianglelefteq S$ is an ideal, so is $\mathfrak{b} := \varphi^{-1}(\mathfrak{a}) \trianglelefteq R$. Let $b \in \mathfrak{b}$. Then $\varphi(b) =: a \in \mathfrak{a}$ by definition. Since $\mathfrak{a} \trianglelefteq_\sigma S$ is a σ-ideal, $\sigma(a) \in \mathfrak{a}$, and since φ is a morphism of σ-rings it follows that $\sigma(a) = \sigma(\varphi(b)) = \varphi(\sigma(b)) \in \mathfrak{a}$. Hence, $\sigma(b) \in \mathfrak{b}$ which implies that $\mathfrak{b}$ is a σ-ideal.

Now let $\mathfrak{a}$ be mixed and $fg \in \mathfrak{b}$. This means by definition of $\mathfrak{b}$, that $\varphi(fg) = \varphi(f)\varphi(g) \in \mathfrak{a}$. Since $\mathfrak{a}$ is mixed, this in turn implies that

$$\varphi(f)\sigma(\varphi(g)) = \varphi(f)\varphi(\sigma(g)) = \varphi(f\sigma(g)) \in \mathfrak{a},$$

which yields $f\sigma(g) \in \mathfrak{b}$, so that $\mathfrak{b}$ is also mixed. The proof for perfect and for reflexive difference ideals is analogous. □

Remark 2.4. Let R be a σ-ring and $\mathfrak{a} \trianglelefteq_\sigma R$ a σ-ideal. We can define a canonical σ-ring structure on the quotient ring $R/\mathfrak{a}$, via $\sigma(r + \mathfrak{a}) := \sigma(r) + \mathfrak{a}$. This is well defined and in particular makes the canonical epimorphism $\tau : R \twoheadrightarrow R/\mathfrak{a}$ a morphism of σ-rings.

Proposition 2.5. *Let R be a σ-ring and $\mathfrak{a} \trianglelefteq_\sigma R$ a σ-ideal. The canonical epimorphism $\tau : R \twoheadrightarrow R/\mathfrak{a}$ induces, in the sense of Lemma 2.3, a bijection between the sets $\{\mathfrak{b} \trianglelefteq_\sigma R/\mathfrak{a}\}$ and $\{\mathfrak{b} \mid \mathfrak{a} \trianglelefteq_\sigma \mathfrak{b} \trianglelefteq_\sigma R\}$. The same holds true, if we restrict both sets to prime, radical and mixed, σ-prime or perfect σ-ideals.*

Proof. See Proposition 1.2.8 of [1]. □

Remark 2.6. Let R be a σ-ring, and $F \subseteq R$ be a subset of R. Any intersection of mixed, radical σ-ideals containing F is also a mixed, radical σ-ideal, which of course contains F. This means that there is a smallest (with respect to inclusion) mixed, radical σ-ideal $\mathfrak{a}$ containing F, namely, the intersection of all such σ-ideals:

$$\mathfrak{a} = \bigcap_{\substack{\mathfrak{b} \trianglelefteq_\sigma R, \\ \mathfrak{b} \text{ radical and mixed}}} \mathfrak{b}.$$

Proof. Let I be an index set and $\mathfrak{b}_i \trianglelefteq_\sigma R$ for all $i \in I$ be mixed, radical σ-ideals. Further, let $\mathfrak{a} := \bigcap_{i \in I} \mathfrak{b}_i$ be the intersection of these. Obviously, $\mathfrak{a}$ is an ideal of R. We will show that it is also a σ-ideal, radical and mixed. If $b \in \mathfrak{b}_i$ for all $i \in I$, then $\sigma(b) \in \mathfrak{b}_i$ for all $i \in I$, since each $\mathfrak{b}_i$ is a σ-ideal. It follows that $\sigma(b) \in \mathfrak{a}$.

Similarly, if $bb' \in \mathfrak{b}_i$ for all $i \in I$, then $b\sigma(b') \in \mathfrak{b}_i$ for all $i \in I$, since each $\mathfrak{b}_i$ is mixed, which implies that $b\sigma(b') \in \mathfrak{a}$. Hence, $\mathfrak{a}$ is mixed.

Finally, if $a \in \sqrt{(}\mathfrak{a})$ there exists an $n \in \mathbb{N}$, such that $a^n \in \mathfrak{a}$. This means that $a^n \in \mathfrak{b}_i$ for all $i \in I$, which implies that $a \in \sqrt{(}\mathfrak{b}_i)$ for all $i \in I$. Since every $\mathfrak{b}_i, i \in I$ is radical, this means that $a \in \mathfrak{b}_i$ for all $i \in I$, and thus $a \in \mathfrak{a}$. This implies that $\mathfrak{a}$ is radical. □

Definition 2.7. *The σ-ideal $\mathfrak{a}$ from Remark 2.6 is called the radical, mixed closure of F. We will denote it by $\{F\}_m$.*

Lemma 2.8. *Let R be a σ-ring and $\mathfrak{a} \trianglelefteq_\sigma R$ be a mixed σ-ideal. Then the radical of $\mathfrak{a}$, $\sqrt{\mathfrak{a}}$, is also mixed.*

Proof. Let $f, g \in R$ be such that $fg \in \sqrt{\mathfrak{a}}$. By definition there exists an $n \in \mathbb{N}_{\geq 1}$ such that $f^n g^n = (fg)^n \in \mathfrak{a}$. Since $\mathfrak{a}$ is mixed, this implies that $f^n \sigma(g^n) = f^n \sigma(g)^n = (f\sigma(g))^n \in \mathfrak{a}$. However, this in turn implies that $f\sigma(g) \in \sqrt{\mathfrak{a}}$, which is what we wanted to show. □

Example 2.9. *Let $\mathbb{Q}$ be the field of rational numbers considered as a constant σ-field and let $R := \mathbb{Q}\{y_1, y_2\}$. Consider the difference ideal $\mathfrak{a} := [y_1 y_2] \trianglelefteq_\sigma R$. We can inductively define a chain*

$$\mathfrak{a}^{\{0\}} := \mathfrak{a}, \ \mathfrak{a}^{\{m+1\}} := [\{f\sigma(g) \mid f, g \in \mathfrak{a}^{\{m\}}\}]$$
$$= [\sigma^k(y_1)\sigma^l(y_2) \mid k, l = 0, 1, \ldots, m+1], \text{ for all } m \in \mathbb{N}_{\geq 1}.$$

This is an infinite properly ascending chain of difference ideals.

Proof. It is enough to only consider the σ-generators of the ideal. We can show the assertion by an induction on m. For $m = 0$ it is obvious.
Assume then that

$$\mathfrak{a}^{\{m\}} = [\sigma^k(y_1)\sigma^l(y_2) \mid k, l = 0, 1, \ldots, m].$$

For $k = 0, \ldots, m$, we know that $\sigma^k(y_1)\sigma^m(y_2) \in \mathfrak{a}^{\{m\}}$. This implies that $\sigma^k(y_1)\sigma^{m+1}(y_2) \in \mathfrak{a}^{\{m+1\}}$. Similarly, $\sigma^m(y_1)\sigma^l(y_2) = \sigma^l(y_2)\sigma^m(y_1) \in \mathfrak{a}^{\{m\}}$ implies that $\sigma^l(y_2)\sigma^{m+1}(y_1) = \sigma^{m+1}(y_1)\sigma^l(y_2) \in \mathfrak{a}^{\{m\}}$, for $l = 0, \ldots, m$. Since these are the only new generators we get through this process, we also get the other inclusion. □

When trying to find $\{\mathfrak{a}\}_m$ for a σ-ideal $\mathfrak{a} \trianglelefteq_\sigma R$ in a difference ring R, it might be tempting to consider $\mathfrak{a}' := \{f\sigma(g) \mid fg \in \mathfrak{a}\}$, or to ensure it is a difference ideal rather, $[\mathfrak{a}']$. The example above shows that this is not enough, as the ideal $[\mathfrak{a}']$ does not have to be mixed in general. However, by iteratively repeating this process and taking the union of σ-ideals obtained this way, we do get a mixed σ-ideal. We will see this in the following lemma, which is very similar to Lemma 3.1 of [10], where the mixed closure is obtained this way.

Lemma 2.10. *Let R be a σ-ring and $F \subseteq R$. Further, let $F' := \{f\sigma(g) \mid fg \in F\}$, and set $F^{\{1\}} := [F']$, $F^{\{n\}} := [F^{\{n-1\}'}]$ for all $n \in \mathbb{N}_{\geq 1}$. Then*

$$\{F\}_m = \sqrt{\bigcup_{n=1}^{\infty} F^{\{n\}}}. \tag{2}$$

This way of obtaining $\{F\}_m$ is called a shuffling processes and has an analogy for perfect σ-ideals (see for example [6], p. 121f.)

Proof. Let $\mathfrak{a} := \bigcup_{n=1}^{\infty} F^{\{n\}}$. It is obvious from the construction that $F \subseteq \mathfrak{a}$. It also holds that $\mathfrak{a}$ is a mixed σ-ideal, since for any $f, g \in \mathfrak{a}$ there exists an $n \in \mathbb{N}_{\geq 1}$ such that $f, g \in F^{\{n\}}$. Hence, $f + g, \sigma(f) \in F^{\{n\}} \subseteq \mathfrak{a}$, as well as $fh \in F^{\{n\}} \subseteq \mathfrak{a}$ for any $h \in R$. Furthermore, for $f, g \in R$ with $fg \in \mathfrak{a}$ there also exists an $n \in \mathbb{N}_{\geq 1}$ such that $fg \in F^{\{n\}}$. Then we have $f\sigma(g) \in F^{\{n+1\}} \subseteq \mathfrak{a}$.

On the other hand, by induction on the iterative steps $F^{\{n\}}$, it follows that for every mixed σ-ideal $\mathfrak{b}$, which contains F, $F^{\{n\}} \subseteq \mathfrak{b}$. Hence, $\mathfrak{a}$ is the smallest mixed σ-ideal containing F.

By Lemma 2.8 we know that $\sqrt{\mathfrak{a}}$ is mixed. This actually shows that $\sqrt{a}$ is indeed the smallest mixed, radical σ-ideal of R containing F, since every such ideal has to contain $\mathfrak{a}$, and thus $\sqrt{\mathfrak{a}}$ as well.

□

Example 2.11. *Let k be a σ-field, and consider $R = k\{y_1\}$. Then the σ-ideal $[y_1] \trianglelefteq_\sigma R$ is mixed, hence equal to its mixed closure (similar to the radical, mixed closure, the smallest mixed σ-ideal containing y_1). The mixed closure of $[y_1] \cdot [y_1]$ is $[y_1\sigma^i(y_1) \mid i \in \mathbb{N}] \not\ni y_1$. One could have expected to get an analogy of the statement in algebraic geometry that $\sqrt{F_1F_2} = \sqrt{F_1} \cap \sqrt{F_2}$. However, this example shows this is not the case for mixed ideals in general. It is however very noteworthy that the ideal $[y_1\sigma^i(y_1) \mid i \in \mathbb{N}] \trianglelefteq_\sigma R$ is not radical. For radical, mixed difference ideals we will get such a statement later (Corollary 3.16).*

A very important result in commutative algebra is the fact that every radical ideal is the intersection of prime ideals. This has an analog for perfect σ-ideals (see Theorem 1.18), as well as for mixed σ-ideals. We will prove the latter, but for this we need a few additional tools. We will first prove a weaker version of the statement, for which we need a few results from commutative algebra:

Lemma 2.12. *Let R be a ring.*

(a) If $S \geq R$ is an overring of R, and $\mathfrak{p}$ is a minimal prime ideal of R, then there exists a minimal prime ideal $\mathfrak{q}$ of S, such that $\mathfrak{p} = \mathfrak{q} \cap R$.

(b) Every radical ideal of R is the intersection of prime ideals. If R is Noetherian, then every radical ideal of R is the intersection of finitely many prime ideals.

(c) If R is Noetherian and $\mathfrak{p} \trianglelefteq R$ is a minimal prime ideal of R, then there exists an element $a \in R$, such that $\mathfrak{p}$ is the annihilator ideal of a, i.e. $\mathfrak{p} = Ann(a) = \{r \in R \mid ra = 0\}$.

Proof.

(a) See [8] Ch. 2, §2.6, Proposition 16.

(b) See [8] Ch. 2, §2.6, Corollary 2 to Proposition 13 and Ch. 2, §4.3, Corollary 3 to Proposition 14.

(c) This is a special case of Theorem 3.1 of [3] for R as an R-module.

□

The following is adapted from the proof given in [1] of Proposition 1.2.28 (here the upcoming Theorem 2.18). It has been worked out in more detail and divided further in an attempt to make this more detailed version of the proof easier to read.

Definition 2.13. *Let R be a difference ring. We say R is* finitely σ-generated over $\mathbb{Z}$*, if there exists a finite set $A \subseteq R$, so that every $f \in R$ can be written as a finite $\mathbb{Z}$-linear combination of σ-powers of elements in A. In other words, for every $f \in R$ there exists an $n \in \mathbb{N}_{\geq 1}$, so that $f \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)]$.*

For any subset $F \subseteq R$ we denote by

$$\mathbb{Z}\{F\} = \{f \in R \mid \text{ there exists an } n \in \mathbb{N} : f \in \mathbb{Z}[F, \sigma(F), \ldots, \sigma^n(F)]\},$$

the set of all elements σ-generated by F over $\mathbb{Z}$.

Proposition 2.14. *Let R be a σ-ring finitely σ-generated over $\mathbb{Z}$. Then, every radical, mixed σ-ideal of R is the intersection of prime σ-ideals.*

Proof. Let $\mathfrak{a} \trianglelefteq_\sigma R$ be a mixed, radical σ-ideal. By Proposition 2.5 there is a bijection between the prime σ-ideals of R containing $\mathfrak{a}$ and those of $R/\mathfrak{a}$. Hence, we can assume without loss of generality that $\mathfrak{a} = [0] \trianglelefteq_\sigma R$, by replacing R with $R/\mathfrak{a}$. This means that we only have to show that the zero ideal $[0]$ of a well-mixed, reduced σ-ring R is the intersection of all its prime σ-ideals. Note that this does not change the fact that R is finitely σ-generated over $\mathbb{Z}$.

Let thus $f \in R$ be such that $f \in \mathfrak{q}$ for all $\mathfrak{q} \trianglelefteq_\sigma R$ prime. We assert that f then has to be 0. Assume this is not the case, i.e. $f \neq 0$. Then, by assumption on R, there is an $n \in \mathbb{N}$, such that $f \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)]$. We can now argue with the usual case of commutative algebra (Lemma 2.12): since

$\mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)]$ is Noetherian and reduced, $(0) \trianglelefteq \mathbb{Z}[A, \ldots, \sigma^n(A)]$ is the intersection of all prime ideals of R. In particular, there exist prime ideals which do not contain f. Let $\mathfrak{q}_0 \trianglelefteq \mathbb{Z}[A, \ldots, \sigma^n(A)]$ be a minimal prime ideal with $f \notin \mathfrak{q}_0$. Since $f \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)] \subset \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+1}(A)]$, by Lemma 2.12, we can find a minimal prime ideal $\mathfrak{q}_1 \trianglelefteq \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+1}(A)]$ such that $\mathfrak{q}_1 \cap \mathbb{Z}[A, \sigma(A), \ldots, \sigma^n(A)] = \mathfrak{q}_0$.

Inductively we find a chain of minimal prime ideals $\mathfrak{q}_i, i \in \mathbb{N}$, $\mathfrak{q}_i \trianglelefteq \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i}(A)]$, with $\mathfrak{q}_{i+1} \cap \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i}(A)] = \mathfrak{q}_i$ for all $i \in \mathbb{N}$. Then $\mathfrak{q} := \bigcup_{i=0}^{\infty} \mathfrak{q}_i$ is a prime ideal of R, with $f \notin \mathfrak{q}$. In fact, $\mathfrak{q}$ is a σ-ideal of R: Let $a \in \mathfrak{q}$. We want to show that $\sigma(a) \in \mathfrak{q}$. By construction of $\mathfrak{q}$ there exists an $i \in \mathbb{N}$, such that $a \in \mathfrak{q}_{i-1} \subseteq \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i-1}(A)]$, which implies that $\sigma(a) \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i}(A)]$. Lemma 2.12 then states that there is an $h \in \mathbb{Z}[A, \sigma(A), \ldots, \sigma^{n+i}(A)]$, such that $\mathfrak{q}_i = \mathrm{Ann}(h)$. It follows that $ah = 0$, and since R is well-mixed, this implies that $\sigma(a)h = 0$. Hence, $\sigma(a) \in \mathfrak{q}_i \subseteq \mathfrak{q}$. This means that $\mathfrak{q}$ is a prime σ-ideal of R not containing f, which contradicts the assumption on f, so that $f = 0$ has to follow. □

For the general case we need yet another tool, the concept of filters:

Definition 2.15. *Let U be a set, and let $F \subseteq Pot(U)$, where $Pot(U)$ denotes the power set on U. Then F is called a* filter *if it satisfies the following axioms:*

- *$U \in F$ and $\emptyset \notin F$.*
- *If $V, W \subseteq U$ with $V \subseteq W$ and $V \in F$, then $W \in F$.*
- *For $V_1, \ldots, V_n \in F$ we have*

$$\bigcap_{i=1}^{n} V_i \in F.$$

A filter F is called an ultrafilter*, if for any $V \subseteq U$ we have $V \in F$ or $U \setminus V \in F$. Note that the first and third axioms together imply that at most one of V and $U \setminus V$ can be in F.*

Remark 2.16. Let U be a set. Then, the set of filters on U is inductively ordered by inclusion. By Zorn's lemma, for every filter F on U there must exist a maximal filter G with respect to inclusion, such that $F \subseteq G$. The maximality of the filter implies that G will be an ultrafilter, since we could otherwise find a new filter G', where G is properly included by adding one of the sets that contradict the ultrafilter property and considering the smallest filter containing this set.

The reason why this concept is useful in our context is the following:

Lemma 2.17. *Let R be a σ-ring, and let M be the set of all σ-subrings of R which are finitely σ-generated over $\mathbb{Z}$. For any fixed subset $F \subseteq R$, consider the set $M_F := \{T \subseteq M \mid \{S \in M \mid F \subseteq S\} \subseteq T\} \subseteq Pot(M)$. Then,*

$$\mathcal{F} := \bigcup_{F \subseteq R \text{ finite}} M_F$$

defines a filter on M. If $\mathcal{G}$ is an ultrafilter containing $\mathcal{F}$, and $P := \prod_{S \in M} S$ with component-wise operations, then the ultrafilter $\mathcal{G}$ defines an equivalence relation on P via $(g_S)_{S \in M} \sim (h_S)_{S \in M} :\Leftrightarrow \{S \in M \mid g_S = h_S\} \in \mathcal{G}$. The set of equivalence classes $P/\mathcal{G} := P/\sim$ has a natural σ-ring structure.

Proof. Let us first show that $\mathcal{F}$ is a filter. For $F \subseteq R$ finite we have

$$\mathbb{Z}\{F\} \in \{S \in M \mid F \subseteq S\} \neq \emptyset.$$

Since $T \supseteq \{S \in M \mid F \subseteq S\}$ for all $T \in M_F$, $\emptyset \notin M_F$ (For $F = \emptyset$ this works as well). That $M \in M_F$ for any $F \subseteq R$ is obvious, as well as that for $T \subseteq U, T \in M_F$ we have $U \in M_F$.

We only need to show that $U, T \in \mathcal{F}$ implies that $U \cap T \in \mathcal{F}$. Let $\hat{U}, \hat{T} \subseteq R$ be finite, such that $U \in M_{\hat{U}}, T \in M_{\hat{T}}$. $\hat{U} \cup \hat{T} \subseteq R$ is also finite and

$$\{S \in M \mid \hat{U} \cup \hat{T} \subseteq S\} \subseteq \{S \in M \mid \hat{U} \subseteq S\} \subseteq U,$$

similarly for T. This means that $U \cap T \in M_{\hat{U} \cup \hat{T}} \subseteq \mathcal{F}$, which finishes the proof that $\mathcal{F}$ is a filter.

Now, consider an ultrafilter $\mathcal{G} \supseteq \mathcal{F}$ and define $\sim$ on P as above. This is an equivalence relation: Let $f \sim g, g \sim h$ for $f, g, h \in P$. This means that $\{S \in M \mid f_S = g_S\} \in \mathcal{G}, \{S \in M \mid g_S = h_S\} \in \mathcal{G}$. However then

$$\{S \in M \mid f_S = g_S\} \cap \{S \in M \mid g_S = h_S\} \subseteq \{S \in M \mid f_S = h_S\} \in \mathcal{G},$$

since $\mathcal{G}$ is a filter. Reflexivity follows from the fact that $M \in \mathcal{G}$, and symmetry is obvious.

We now only need to show that we have a well-defined σ-ring structure on $P/\sim$. Consider $f, f' \in P$ with $f \sim f'$. For all $S \in M$ with $f_S = f'_S$ we have $\sigma(f)_S = \sigma(f')_S$. Then $\{S \in M \mid \sigma(f)_S = \sigma(f')_S\} \supseteq \{S \in M \mid f_S = f'_S\} \in \mathcal{G}$, by assumption, and since $\mathcal{G}$ is a filter, this means that

$$\{S \in M \mid \sigma(f)_S = \sigma(f')_S\} \in \mathcal{G}.$$

Hence $\sigma(f) \sim \sigma(f')$. That $+$ and $\cdot$ are also well-defined can be proven in an analogous fashion. □

We can now turn our attention to the generalization of Proposition 2.14.

Theorem 2.18. *Let R be a σ-ring and $F \subseteq R$ be a subset of R. Then,*

$$\{F\}_m = \bigcap_{\substack{F \subseteq \mathfrak{p} \trianglelefteq_\sigma R \\ \mathfrak{p} \text{ prime}}} \mathfrak{p}.$$

In particular, every radical, mixed σ-ideal of R is the intersection of prime σ-ideals.

Proof. It suffices to show that every radical, mixed σ-ideal of R is the intersection of prime σ-ideals. Indeed, since prime σ-ideals are radical and mixed, it is clear that $\{F\}_m \subseteq \mathfrak{p}$ for every prime $\mathfrak{p} \trianglelefteq_\sigma R$ with $F \subseteq \mathfrak{p}$. Together with the fact that every radical, mixed σ-ideal of R is the intersection of prime σ-ideals, this gives the representation

$$\{F\}_m = \bigcap_{\substack{F \subseteq \mathfrak{p} \trianglelefteq_\sigma R \\ \mathfrak{p} \text{ prime}}} \mathfrak{p}.$$

Now, by the same argument as in the beginning of the proof of Proposition 2.14, it is enough to prove in the case that R is well-mixed and reduced, that the intersection of all prime σ-ideals of R is $[0]$. Let $0 \neq f \in R$. We will construct a prime σ-ideal $\mathfrak{q}$ of R, which does not contain f:

Let $P/\mathcal{G}$ be the difference ring as in Lemma 2.17. Consider the mapping $\varphi : R \to P/\mathcal{G}, g \mapsto (g_S)_{S \in M}$ with $(g_S) = g$ for all $S \in M$ with $g \in S$ and $(g_S) = 0$ for $g \notin S$. It is, in fact, $\{S \in M \mid g \in S\} \in M_{\{g\}}$ (with $M_{\{g\}}$ as in Lemma 2.17). It follows from this that the image of the mapping onto $P/\mathcal{G}$ is independent of the (g_S) for $g \notin S$, as any other choice of these would be in the same equivalence class as the image described above. It follows that φ is a well-defined morphism of σ-rings.

From Proposition 2.14 we know that for every $S \in M$, there exists a prime σ-ideal $\mathfrak{p}_S \trianglelefteq_\sigma S$, such that $f \notin \mathfrak{p}_S$. We define $\mathfrak{p} \subseteq P/\mathcal{G}$ as the set of all equivalence classes of elements $(g_S)_{S \in M}$, such that $\{S \in M \mid g_S \in \mathfrak{p}_S\} \in \mathcal{G}$. For $[(g_S)_{S \in M}]_\sim, [(h_s)_{S \in M}]_\sim \in \mathfrak{p}$ we have

$$\mathcal{G} \ni \{S \in M \mid g_S \in \mathfrak{p}_S\} \cap \{S \in M \mid h_S \in \mathfrak{p}_S\} \subseteq \{S \in M \mid g_S + h_S \in \mathfrak{p}_S\} \in \mathcal{G},$$

since $\mathcal{G}$ is a filter. Similar arguments for $\sigma(g), gh$ for $h \in P/\mathcal{G}$ show that $\mathfrak{p}$ is indeed a σ-ideal. $\mathfrak{p}$ is also prime since $\mathcal{G}$ is an ultrafilter: Let $g, h \in P$ with $\{S \in M \mid g_S h_S \in \mathfrak{p}_S\} \in \mathcal{G}$. If $[g]_\sim \notin \mathfrak{p}$, then $V := \{S \in M \mid g_S \in \mathfrak{p}_S\} \notin \mathcal{G}$. Since $\mathcal{G}$ is an ultrafilter, this means that $M \setminus V \in \mathcal{G}$. However,

$$\mathcal{G} \ni (M \setminus V) \cap \{S \in M \mid g_S h_S \in \mathfrak{p}_S\} \subseteq \{S \in M \mid h_S \in \mathfrak{p}_S\} \in \mathcal{G},$$

which means that $[h]_\sim \in \mathfrak{p}$. The preimage of a prime σ-ideal, $\mathfrak{q} := \varphi^{-1}(\mathfrak{p}) \trianglelefteq_\sigma R$ is also prime (see Lemma 2.3). By construction, $[\varphi(f)]_\sim \notin \mathfrak{p}$, which means that $f \notin \varphi^{-1}(\mathfrak{p})$, as desired.

□

2.2 An Analog of the Cohn Topology

Definition 2.19. *Let R be a σ-ring. We denote the set of all prime σ-ideals of R by* $\mathrm{Spec}_m^\sigma(R) := \{\mathfrak{p} \trianglelefteq_\sigma R \mid \mathfrak{p} \text{ prime }\}$. *Similarly, we denote the set of σ-prime ideals by* $\mathrm{Spec}^\sigma(R) := \{\mathfrak{p} \trianglelefteq_\sigma R \mid \mathfrak{p} \ \sigma\text{-prime }\} \subseteq \mathrm{Spec}_m^\sigma(R)$.

Remark 2.20. As is the case with $\mathrm{Spec}^\sigma(R)$, it can be the case that $\mathrm{Spec}_m^\sigma(R) = \emptyset$. For example, let R be a σ-ring, and consider the σ-ring $R \oplus R$ with $\sigma((r,s)) := (\sigma(s), \sigma(r))$. We will show that this ring has no prime σ-ideals. Let $\mathfrak{p} \trianglelefteq R$ prime. Then $0 = (1,0)(0,1) \in \mathfrak{p}$, which means that either $(1,0) \in \mathfrak{p}$ or $(0,1) \in \mathfrak{p}$. Then $R \oplus 0 \subseteq \mathfrak{p}$ or $0 \oplus R \subseteq \mathfrak{p}$. If we assume that $\mathfrak{p}$ is a σ-ideal then this implies that $R \oplus R \subseteq \mathfrak{p}$, which by definition cannot be.

In algebraic geometry, one usually considers $\mathrm{Spec}(R)$ as a topological space with a topology called the Zariski topology. This has an analog for $\mathrm{Spec}^\sigma(R)$, usually called the Cohn topology. Here we will develop a further analog of both, which we will define on $\mathrm{Spec}_m^\sigma(R)$ and will be closely related to radical, mixed σ-ideals, as we shall see by its many properties.

Definition 2.21. *Let R be a σ-ring and $F \subseteq R$ be a subset of R. We set* $\mathcal{V}_m(F) := \{\mathfrak{p} \in \mathrm{Spec}_m^\sigma(R) \mid F \subseteq \mathfrak{p}\}$. *If F has only one element f, we write $\mathcal{V}_m(f)$ for $\mathcal{V}_m(F)$.*

Lemma 2.22. *Let R be a σ-ring. Then we have:*

(a) $\mathcal{V}_m((0)) = \mathrm{Spec}_m^\sigma(R)$, *and* $\mathcal{V}_m(R) = \emptyset$.

(b) For any two ideals $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ *we have* $\mathcal{V}_m(\mathfrak{a}) \cup \mathcal{V}_m(\mathfrak{b}) = \mathcal{V}_m(\mathfrak{a} \cap \mathfrak{b})$.

(c) For any family of ideals $(\mathfrak{a}_i)_{i \in I}$ *for an index set I, we have*

$$\bigcap_{i \in I} \mathcal{V}_m(\mathfrak{a}_i) = \mathcal{V}_m(\sum_{i \in I} \mathfrak{a}_i).$$

Proof.

(a) We have $(0) \subseteq \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}_m^\sigma(R)$, as well as $R \not\subseteq \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}_m^\sigma(R)$.

(b) Let $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ be two ideals in R. Then $\mathcal{V}_m(\mathfrak{a}) \cup \mathcal{V}_m(\mathfrak{b}) \subseteq \mathcal{V}_m(\mathfrak{a} \cap \mathfrak{b})$, since for $\mathfrak{p} \trianglelefteq_\sigma R$ prime $\mathfrak{a} \subseteq \mathfrak{p}$, it follows that $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, and similarly for $\mathfrak{b}$. On the other hand, let $\mathfrak{p} \trianglelefteq_\sigma R$ prime with $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, and $\mathfrak{a} \not\subseteq \mathfrak{p}$ (otherwise $\mathfrak{p} \in \mathcal{V}_m(\mathfrak{a})$ and we are done). Then there exists an $f \in \mathfrak{a}$, $f \notin \mathfrak{p}$. For any $g \in \mathfrak{b}$, it follows that $fg \in \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this implies that $g \in \mathfrak{p}$. Hence, $\mathfrak{b} \subseteq \mathfrak{p}$, which concludes the proof.

(c) Let $(\mathfrak{a}_i)_{i \in I}$ be a family of ideals of R. Then

$$\mathfrak{p} \in \bigcap_{i \in I} \mathcal{V}_m(\mathfrak{a}_i) \Leftrightarrow \mathfrak{a}_i \subseteq \mathfrak{p} \text{ for all } i \in I \Leftrightarrow \mathfrak{p} \in \mathcal{V}_m(\sum_{i \in I} \mathfrak{a}_i).$$

□

Remark 2.23. Since for a σ-ring R any prime σ-ideal of R is radical and mixed, then for any $F \subseteq R$, and any prime σ-ideal $\mathfrak{p} \trianglelefteq_\sigma R$ with $F \subseteq \mathfrak{p}$ we have $(F) \subseteq [F] \subseteq \{F\}_m \subseteq \mathfrak{p}$. In particular, this means that

$$\mathcal{V}_m(F) = \mathcal{V}_m((F)) = \mathcal{V}_m([F]) = \mathcal{V}_m(\{F\}_m).$$

Definition 2.24. *Let R be a σ-ring. We define a topology on $\operatorname{Spec}_m^\sigma(R)$ by letting $A \subseteq \operatorname{Spec}_m^\sigma(R)$ be closed if $A = \mathcal{V}_m(\mathfrak{a})$ for an ideal $\mathfrak{a} \trianglelefteq R$, or equivalently, by defining a set to be open, if it is a complement of such a $\mathcal{V}_m(\mathfrak{a})$. This is a well-defined topology thanks to Lemma 2.22. For $f \in R$ we set*

$$\sigma\text{-}\mathrm{D}_m(f) := \operatorname{Spec}_m^\sigma(R) \setminus \mathcal{V}_m(f).$$

$\sigma\text{-}\mathrm{D}_m(f)$ is the complement of a closed set, and hence, open. We call the sets of the form $\sigma\text{-}\mathrm{D}_m(f) \subseteq \operatorname{Spec}_m^\sigma(R)$ basic open subsets *of $\operatorname{Spec}_m^\sigma(R)$.*

From here on, if not explicitly stated otherwise, when referring to topological concepts on $\operatorname{Spec}_m^\sigma(R)$ we will be referring to the topology just defined.

Remark 2.25. From its definition it is clear that $\operatorname{Spec}_m^\sigma(R) \subseteq \operatorname{Spec}(R) := \{I \trianglelefteq R \mid I \text{ prime}\}$. Since Lemma 2.22 does not require the ideals to be difference ideals, it is easy to conclude that in fact the topology on $\operatorname{Spec}_m^\sigma(R)$ is just the topology induced by restriction of the Zariski topology to $\operatorname{Spec}_m^\sigma(R)$. The same argument can be made to see that the Cohn topology in turn, defined on $\operatorname{Spec}^\sigma(R) = \{\mathfrak{p} \trianglelefteq_\sigma R \mid \mathfrak{p} \ \sigma\text{-prime}\ \} \subseteq \operatorname{Spec}_m^\sigma(R)$, is also the restriction of the topology defined on $\operatorname{Spec}_m^\sigma(R)$.

Definition 2.26. *Let X be a topological space.*

(a) *We say that X is* irreducible*, if $X = X_1 \cup X_2$ with X_1, X_2 closed implies that $X = X_1$ or $X = X_2$. $X_1 \subseteq X$ is called* irreducible*, if it is an irreducible topological space with the topology induced by the restriction to X_1.*

(b) *Let $Y \subseteq X$ be closed. We say that a point $f \in Y$ is a* generic point *of Y, if $\overline{\{f\}} = Y$, where for $A \subseteq X$, $\overline{A}$ denotes the closure of A.*

Proposition 2.27. *Let R be a σ-ring. We have:*

(a) *The mapping*

$$\{\mathfrak{a} \trianglelefteq_\sigma R \mid \mathfrak{a} \text{ mixed, radical } \} \to \{A \subseteq \operatorname{Spec}_m^\sigma(R) \mid A \text{ closed } \}, \mathfrak{a} \mapsto \mathcal{V}_m(\mathfrak{a})$$

is bijective and order-reversing.

(b) *Let $F \subseteq R$ be a subset of R. Then $\mathcal{V}_m(F)$ is irreducible, if and only if $\{F\}_m$ is prime.*

(c) $\operatorname{Spec}_m^\sigma(R)$ *is quasi-compact.*

(d) *The basic open sets $\{\sigma\text{-}\operatorname{D}_m(f) \mid f \in R\}$ form a basis for the topology on $\operatorname{Spec}_m^\sigma(R)$.*

(e) *Every irreducible closed subset Y of $\operatorname{Spec}_m^\sigma(R)$ has a unique generic point y.*

Proof.

(a) That the mapping is order-reversing is obvious. The injectivity follows from the fact that by Theorem 2.18 $\mathfrak{a} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p} \in \operatorname{Spec}_m^\sigma(R)} \mathfrak{p}$. By Remark 2.23 we obtain the surjectivity, since $\mathcal{V}_m(\mathfrak{a}) = \mathcal{V}_m(\{\mathfrak{a}\}_m)$.

(b) Since $\mathcal{V}_m(F) = \mathcal{V}_m(\{F\}_m)$, we can assume without loss of generality, that $F \trianglelefteq_\sigma R$ is a radical, mixed σ-ideal. For the first implication, "$\Leftarrow$", let $F \trianglelefteq_\sigma R$ be prime, and $\mathcal{V}_m(F) = \mathcal{V}_m(\mathfrak{a}) \cup \mathcal{V}_m(\mathfrak{b})$ with radical, mixed σ-ideals $\mathfrak{a}, \mathfrak{b}$. Assume that $\mathcal{V}_m(F) \not\subseteq \mathcal{V}_m(\mathfrak{a})$. Then by (a), $\mathfrak{a} \not\subseteq F$, so there exists an $a \in \mathfrak{a}$, with $a \notin F$. For any $b \in \mathfrak{b}$ we then have $ab \in \mathfrak{p}$ for all $\mathfrak{p} \in \mathcal{V}(F) = \mathcal{V}_m(\mathfrak{a}) \cup \mathcal{V}_m(\mathfrak{b})$, and with Theorem 2.18 we get $ab \in F = \bigcap_{\mathfrak{p} \in \mathcal{V}_m(F)} \mathfrak{p}$. By assumption, F is prime and $a \notin F$, which implies that $b \in F$. However, this means that $\mathfrak{b} \subseteq F$, and thus $\mathcal{V}_m(F) \subseteq \mathcal{V}_m(\mathfrak{b})$, which shows the irreducibility.
Now, for the other implication, "$\Rightarrow$", assume that $\mathcal{V}_m(F)$ is irreducible, and let $a, b \in R$ with $ab \in F$. Consider $F \subseteq \mathfrak{p} \in \mathcal{V}_m(F)$. Then $ab \in \mathfrak{p}$,

which means that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, since $\mathfrak{p}$ is prime. This implies that $\mathfrak{p} \in \mathcal{V}_m(\{a\}_m) \cup \mathcal{V}_m(\{b\}_m)$, which in turn implies that

$$\mathcal{V}_m(F) \subseteq \mathcal{V}_m(\{a\}_m) \cup \mathcal{V}_m(\{b\}_m).$$

Now, by assumption, $\mathcal{V}_m(F)$ is irreducible, and thus it has to be that $\mathcal{V}_m(F) \subseteq \mathcal{V}_m(\{a\}_m)$ or $\mathcal{V}_m(F) \subseteq \mathcal{V}_m(\{b\}_m)$. By the bijectivity of the mapping in (a) this means that $a \in F$ or $b \in F$.

(c) Let $\mathcal{V}_m(\mathfrak{a}_i)_{i\in I}$ be a family of closed sets, $\mathfrak{a}_i \trianglelefteq_\sigma R$ mixed, radical for all $i \in I$, satisfying that $\bigcap_{i\in J} \mathcal{V}_m(a_i) \neq \emptyset$ for every finite $J \subseteq I$. By going to the complement of open sets, quasi-compactness is equivalent to the implication that $\bigcap_{i\in I} \mathcal{V}_m(a_i) \neq \emptyset$. By Lemma 2.22 we see that

$$\bigcap_{i\in I} \mathcal{V}_m(\mathfrak{a}_i) = \mathcal{V}_m(\sum_{i\in I} \mathfrak{a}_i).$$

Assume that $\mathcal{V}_m(\sum_{i\in I} \mathfrak{a}_i) = \emptyset$. By Theorem 2.18 this means that $\{\sum_{i\in I} \mathfrak{a}_i\}_m = R$. In particular, $1 \in \{\sum_{i\in I} \mathfrak{a}_i\}_m$. By the construction in Lemma 2.10 (and with the notation used there), this means that there has to be an $n \in \mathbb{N}_{\geq 1}$, so that $1 \in (\sum_{i\in I} \mathfrak{a}_i)^{\{n\}}$. In particular, this means that 1 can be written as a σ-polynomial in finitely many elements from finitely many $\mathfrak{a}_i$. This implies that there exists a $J \subseteq I$ finite, such that $1 \in (\sum_{i\in J} \mathfrak{a}_i)^{\{n\}}$. This in turn means that

$$\mathcal{V}_m(\sum_{i\in J} \mathfrak{a}_i) = \cap_{i\in J} \mathcal{V}_m(\mathfrak{a}_i) = \emptyset,$$

a contradiction.

(d) For an open subset $U \subseteq \mathrm{Spec}_m^\sigma(R)$ there exists by definition an $\mathfrak{a} \trianglelefteq_\sigma R$, such that $U = \mathrm{Spec}_m^\sigma(R) \setminus \mathcal{V}_m(\mathfrak{a})$. We can then write U as a union of basic open sets as follows:

$$U = \bigcup_{a\in\mathfrak{a}} \sigma\text{-}\,\mathrm{D}_m(a).$$

(e) By (b), an irreducible closed subset A of $\mathrm{Spec}_m^\sigma(R)$ has the form $A = \mathcal{V}_m(\mathfrak{p})$, for $\mathfrak{p} \trianglelefteq_\sigma R$ prime. This prime σ-ideal $\mathfrak{p}$ is the unique generic point of A. To see this, consider the closure of $\mathfrak{p}$:

$$\overline{\{\mathfrak{p}\}} = \bigcap_{\{\mathfrak{p}\}\subseteq\mathcal{V}_m(F)} \mathcal{V}_m(F).$$

From the definition of $\mathcal{V}_m(F)$ we know that $\{\mathfrak{p}\} \subseteq \mathcal{V}_m(F)$ if and only if $F \subseteq \mathfrak{p}$. By Lemma 2.22 (c) and the obvious fact that we can restrict the intersection to σ-ideals, we thus get

$$\overline{\{\mathfrak{p}\}} = \bigcap_{F \subseteq \mathfrak{p}} \mathcal{V}_m(F) = \mathcal{V}_m(\sum_{F \subseteq \mathfrak{p}, F \trianglelefteq_\sigma R} F) = \mathcal{V}_m(\mathfrak{p}) = A.$$

□

2.3 An alternative proof of Theorem 2.18

There is an alternative proof of Theorem 2.18 without ultrafilters, just using difference algebraic arguments. We will develop it here additionally.

Definition 2.28. *Let R be a difference ring and $\mathfrak{a} \trianglelefteq_\sigma R$ be a mixed σ-ideal of R. Further, let $f \in R \setminus \mathfrak{a}$. We set*

$$(\mathfrak{a} : f) := \{g \in R \mid gf \in \mathfrak{a}\} \subseteq R$$

Lemma 2.29. *Let R be a σ-ring, $\mathfrak{a} \trianglelefteq_\sigma R$ a mixed σ-ideal, $f \notin \mathfrak{a}$. Then $(\mathfrak{a} : f)$ is a mixed σ-ideal of R, which contains $\mathfrak{a}$. If $\mathfrak{a}$ is radical(prime), then $(\mathfrak{a} : f)$ is radical(prime) as well.*

Proof. We will only prove the difference-algebraic statements, since the rest of the assertion is standard in commutative algebra. Let $a \in (\mathfrak{a} : f), r \in R$.

Since $\mathfrak{a}$ is mixed and $af \in \mathfrak{a}$ it follows that $\sigma(a)f \in \mathfrak{a}$, which in turn means that $\sigma(a) \in (\mathfrak{a} : f)$. This shows that $(\mathfrak{a} : f)$ is a difference ideal. To see that $(\mathfrak{a} : f)$ is mixed, let $g, h \in R$ with $gh \in (\mathfrak{a} : f)$. Then we know that $(gh)f = (gf)h \in \mathfrak{a}$. Since $\mathfrak{a}$ is mixed, this implies that $(gf)\sigma(h) = (g\sigma(h))f \in \mathfrak{a}$, from which $g\sigma(h) \in (\mathfrak{a} : f)$ follows immediately by definition.

□

Lemma 2.30. *Let R be a difference ring and let $\emptyset \neq U \subset R$ be a multiplicatively closed subset of R. Then a mixed difference ideal $\mathfrak{a} \subset R$ which is maximal (with respect to inclusion) in the class of mixed difference ideals not meeting U, i.e. such that $\mathfrak{a} \cap U = \emptyset$, is prime.*

Proof. Let $\mathfrak{a} \subset R$ be a maximal mixed difference ideal not meeting U, and assume that $\mathfrak{a}$ is not prime. Then there exist $f, g \in R$, such that $f, g \notin \mathfrak{a}$, but $fg \in \mathfrak{a}$. $\mathfrak{a}$ is a proper subset of the σ-ideal $(\mathfrak{a} : f)$, since $g \in (\mathfrak{a} : f)$ by definition, but $g \notin \mathfrak{a}$ by assumption. By Lemma 2.29 $(\mathfrak{a} : f)$ is mixed, and due to the maximality of $\mathfrak{a}$, there exists an $u \in U \cap (\mathfrak{a} : f)$.

We distinguish two cases: First, assume that $f \in U$. We know that $uf \in \mathfrak{a}$, but by assumption $f \in U$ and U is multiplicatively closed, which implies that $fu \in U \cap \mathfrak{a}$, a contradiction.

Now consider the case that $f \notin U$. Since $(\mathfrak{a} : f) \supsetneq \mathfrak{a}$, this again implies that there exists an $u \in U \cap (\mathfrak{a} : f)$. By definition of $(\mathfrak{a} : f)$, we know that $uf \in \mathfrak{a}$, as well as $u, f \notin \mathfrak{a}$. We can now apply the arguments as in the first case by considering $f' = u, g' = f$. □

We are now ready to give an alternative proof of Theorem 2.18.

Theorem 2.18. Let R be a difference ring and $F \subseteq R$ be a subset of R. Then

$$\{F\}_m = \bigcap_{F \subseteq \mathfrak{p} \trianglelefteq_\sigma R, \mathfrak{p} \text{ prime}} \mathfrak{p}.$$

Proof. The inclusion "$\subseteq$" is obvious, since prime difference ideals are radical and mixed (see Remark 2.2). For the inclusion "$\supseteq$", let $g \in R$, $g \notin \{F\}_m$, and consider the multiplicatively closed set $U = \{g^k \mid k \in \mathbb{N}_{\geq 1}\} \subset R$. $\{F\}_m \cap U = \emptyset$ since $\{F\}_m$ is radical. By Lemma 2.30, any maximal mixed difference ideal $\mathfrak{p}$ that is disjoint with U is a prime difference ideal. We can always find a maximal mixed difference ideal over $\{F\}_m$ by Zorn's Lemma, since the union of any ascending chain of mixed difference ideals is always a mixed difference ideal. In particular, since $\{F\}_m$ is a mixed difference ideal disjoint from U, this implies that there exists a prime difference ideal $\mathfrak{p} \supseteq \{F\}_m$, such that $g \notin \mathfrak{p}$, which in turn implies that $g \notin \bigcap_{\mathfrak{a} \subseteq \mathfrak{p} \trianglelefteq_\sigma R, \mathfrak{p} \text{ prime}} \mathfrak{p}$. By taking the contraposition of this we get the desired inclusion. □

3 Mixed Difference Varieties

In this section we will introduce a new concept of difference varieties. We will do so in a way that they correspond with the topology on $\mathrm{Spec}_m^\sigma(R)$ which we defined in the previous section. This section will again be based on M. Wibmer's lecture notes [1], where this is worked out for the analogous case of perfect σ-ideals.

3.1 Mixed Difference Varieties

Definition 3.1. *Let A be a σ-ring. If A is an integral domain, we call A an* integral σ-ring. *If, additionally, the endomorphism σ on A is injective, then we call A a* σ-domain.

Remark 3.2. Let A be a σ-domain. Then its field of fractions $\mathrm{Quot}(A) =: k$ is a σ-field: For $\frac{r}{s} \in k$ we define $\sigma(\frac{r}{s}) := \frac{\sigma(r)}{\sigma(s)}$. Since σ is injective, we have $\sigma(s) \neq 0$ for $s \neq 0$, which implies that σ is well defined on k. By this argument, we see that - in general - for an integral σ-ring A, $\mathrm{Quot}(A)$ is a σ-field (in this natural way), if and only if A is a σ-domain.

Our main purpose, in a first instance at least, is to investigate the properties of solutions to difference equations. We will start with a σ-field k and look for solutions (zeros) of some σ-polynomial p over k, i.e. $p \in k\{y_1, \dots, y_n\}$. In general it will be a set of σ-polynomials $F \subseteq k\{y_1, \dots, y_n\}$ that we will study. For this, we want to define a new concept of σ-varieties. However, we cannot mimic the usual approach from algebraic geometry, where one would work over the algebraic closure of k. The next remark shows why.

Remark 3.3. Consider the constant σ-field $\mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2})$, with $\sigma(\sqrt{2}) = \sqrt{2}$; $L = \mathbb{Q}(\sqrt{2}), \sigma(\sqrt{2}) = -\sqrt{2}$. Both K and L are σ-field extensions of $\mathbb{Q}$, but there cannot be a further extension $\mathbb{Q} \leq M$ of σ-fields, such that $K, L \leq M$ are both (isomorphic to) σ-subfields of M. To see this, assume there was such an M. Then the set $\{a \in M \mid a^2 - 2 = 0\}$ has exactly two elements, which we will call $\sqrt{2}, -\sqrt{2}$ (since $\sqrt{2} + (-\sqrt{2}) = 0$). But $\sqrt{2} \in K$ has to be mapped to one of these two in any embedding. The same holds true for $\sqrt{2} \in L$, which already yields the contradiction, since in M either $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2}) = -\sqrt{2}$.

To avoid this problem, we will define our new, mixed σ-varieties as functors. For this, we will need a few category-theoretic definitions:

Definition 3.4. *Let k be a σ-field. The category of all σ-ring extensions A of k (i.e. such that $k \subseteq A$ is a sub σ-ring of A) is denoted by* σ-$\mathbf{ring}_k$.

The morphisms are defined as follows: For $B, C \in \sigma\textbf{-ring}_k$ we say that a morphism of σ-rings $\varphi : B \to C$ is a morphism of σ-ring extensions of k, if and only if $\varphi_{|k} = id_k$. The subcategory which arises from restricting the object class to integral σ-rings, the category of integral σ-ring extensions of *k, we denote by $\sigma\textbf{-int}_k$.*

Because k is a field, any non-trivial morphism of σ-rings from k to a k-σ-algebra is injective. This means that the category $\sigma\textbf{-ring}_k$ is equivalent to that of k-σ-algebras, the only difference is if k is a subset or just isomorphic to one. Now we are ready to define the new concept of σ-varieties of σ-rings, with mixed σ-ideals in mind:

Definition 3.5. *Let k be a σ-field and $B \in \sigma\textbf{-int}_k$ an integral σ-overring of k. Further let $F \subseteq k\{y_1, \ldots, y_n\}$ be a set of σ-polynomials over k. Then we define $\mathbb{V}_B(F) := \{b \in B^n \mid f(b) = 0$ for all $f \in F\}$. A functor $X : \sigma\textbf{-int}_k \to \textbf{Set}$, for which there exists a set $F \subseteq k\{y_1, \ldots, y_n\}$, such that $X(B) = \mathbb{V}_B(F)$ for all $B \in \sigma\textbf{-int}_k$, we denote as a* mixed σ-variety over *k, or a k-σ-*m-variety*. *Here,* **Set** *denotes the usual category of sets with mappings as morphisms. We also write $X := \mathbb{V}(F)$ as a short notation for this functor.*

If $A, B \in \sigma\textbf{-int}_k$ are two integral σ-overrings of k, and $\varphi : A \to B$ is a morphism in $\sigma\textbf{-int}_k$, then φ induces a map from $\mathbb{V}_A(F) \to \mathbb{V}_B(F), a \mapsto \varphi(a)$, which is why X above is indeed a functor.

We can compare this definition to the definition of difference varieties in Section 1. The difference lies in the category considered for the codomain of the functor, where instead of σ-fields over k we take $\sigma\textbf{-int}_k$. This begs the question what would happen if we considered yet another category instead, for example only allowing the ring to be perfectly σ-reduced, or a σ-domain. It can be shown that the category of difference varieties yielded by those definitions is equivalent to the standard definition of difference varieties. We will prove this at the end of this section when we have the necessary tools to do it.

Definition 3.6. *Let k be a σ-field and $X : \sigma\textbf{-int}_k \to \textbf{Set}$ be a k-σ-m-variety. We say a subfunctor $Y \subseteq X$ is a* σ-m-subvariety *of X, if Y is a k-σ-m-variety itself.*

Remark 3.7. Let k be a σ-field and X be a k-σ-m-variety. Not every subfunctor of X is a σ-m-subvariety. Consider the functor $X = \mathbb{V}(0)$, for $\{0\} \subset k\{y_1\}$. For $B \in \sigma\textbf{-int}_k$ we denote by $B^* = \{b \in B \mid b$ invertible $\}$ the set of units of B. Then for $B \in \sigma\textbf{-int}_k$, $B \mapsto B^*$ is a subfunctor Y of X (since $B^* \subset B$ for all $B \in \sigma\textbf{-int}_k$ and morphisms of rings always map units

to units). However, Y is not a σ-m-variety: there exists no $F \subseteq k\{y_1\}$, such that $\mathbb{V}_B(F) = B^*$ for all $B \in \sigma\text{-}\mathbf{int}_k$. Indeed, assume there was such an F, and let $0 \neq f \in F$. Then $f(b) = 0$ for all $b \in B^*$ and for all $B \in \sigma\text{-}\mathbf{int}_k$. In particular, for $B = k\langle y_1 \rangle = \mathrm{Quot}(k\{y_1\}) \in \sigma\text{-}\mathbf{int}_k$ we get the that $f(y_1) = f = 0,\ y_1 \in k\langle y_1 \rangle^*$, a contradiction.

Definition 3.8. *Let $X = \mathbb{V}(F)$ be a σ-m-variety over the σ-field k, $F \subseteq k\{y_1, \ldots, y_n\}$. Then we set*

$$\mathbb{I}_m(X) := \{f \in k\{y_1, \ldots, y_n\} \mid f(b) = 0 \text{ for all } b \in \mathbb{V}_B(F),\ B \in \sigma\text{-}\mathbf{int}_k\}.$$

Example 3.9. *Let k be a σ-field and let $\{0\} =: F \subseteq k\{y_1, \ldots, y_n\}$. Then a σ-m-variety X is defined by F, $X(B) := \mathbb{V}_B(F)$ for all $B \in \sigma\text{-}\mathbf{int}_k$ with the property that $X(B) = B^n$ for all $B \in \sigma\text{-}\mathbf{int}_k$. For every $G \subseteq k\{y_1, \ldots, y_n\}$ the σ-m-variety given by $Y : B \mapsto \mathbb{V}_B(G)$ is a σ-m-subvariety of X.*

Definition 3.10. *The σ-m-variety X defined in Example 3.9 is called the* affine n-space*, and is denoted by $\mathbb{A}^n_k$, or simply $\mathbb{A}^n$, whenever k is clear from the context. Since for every $G \subseteq A\{y_1, \ldots, y_n\}$ the σ-m-variety given by $Y : B \mapsto \mathbb{V}_B(G)$ is a σ-m-subvariety of X, we write $Y \subseteq \mathbb{A}^n$ as a shorthand for the former.*

We note that 0 is in any (radical, mixed, difference) ideal, so it is not surprising that every σ-m-variety is a σ-m-subvariety of $\mathbb{V}(0)$. This "intuition" will be made more concrete later on.

Since we have this functorial definition, we have, in principle, a whole proper class of solutions for most systems of difference equations. We want to have some sort of equivalence relation between solutions to group them up in a reasonable manner.

Definition 3.11. *Let k be a σ-field, $B, C \in \sigma\text{-}\mathbf{int}_k$. Further let $F \subseteq k\{y_1, \ldots, y_n\}$ be a system of difference equations and $b \in B^n, c \in C^n$ be solutions of F, i.e. $b \in \mathbb{V}_B(F), c \in \mathbb{V}_C(F)$. We say that b and c are* equivalent *if the mapping $b \mapsto c$ is a well-defined isomorphism between the integral σ-rings $k\{b\}$ and $k\{c\}$ (as elements of $\sigma\text{-}\mathbf{int}_k$).*

Remark 3.12. Recall the definition of equivalence of solutions for σ-varieties in Section 1, where two solutions a, b of a system of difference equation over a difference field k are said to be equivalent if the σ-field extensions $k\langle a \rangle$ and $k\langle b \rangle$ are isomorphic as σ-field extensions of k via $a \mapsto b$. This is in accordance with Definition 3.11, i.e. solutions in difference field extensions are equivalent if and only if they are equivalent as solutions in integral σ-overrings in the sense of Definition 3.11.

Proof. Assume that there exist σ-field extensions $k \leq A, B$, and elements $a \in A^n$, $b \in B^n$ such that a and b are equivalent as solutions in the sense of Definition 3.11. Since A, B are σ-fields, it means that $k\{a\}$ and $k\{b\}$ are σ-domains, and $k\langle a\rangle, k\langle b\rangle$ have the "canonical" difference structure induced by $k\{a\}, k\{b\}$ (see Remark 3.2). Let $\varphi : k\{a\} \to k\{b\}, a \mapsto b$ be an isomorphism of integral σ-ring extensions of k. Then we can define

$$\tilde{\varphi} : k\langle a\rangle \to k\langle b\rangle, \frac{x}{y} \mapsto \frac{\varphi(x)}{\varphi(y)}.$$

This is a well-defined isomorphism of σ-field extensions of k, since:

$$\tilde{\varphi}\left(\sigma\left(\frac{x}{y}\right)\right) = \tilde{\varphi}\left(\frac{\sigma(x)}{\sigma(y)}\right) = \frac{\varphi(\sigma(x))}{\varphi(\sigma(y))} = \frac{\sigma(\varphi(x))}{\sigma(\varphi(y))} = \sigma\left(\tilde{\varphi}\left(\frac{x}{y}\right)\right).$$

The converse implication is obvious. □

Example 3.13. *In the two σ-field extensions of $\mathbb{Q}$ in Remark 3.3 we have two solutions of the (algebraic) polynomial $y^2 - 2$, which represent two non-equivalent solutions in the difference algebraic sense, since the σ-fields $\mathbb{Q}(\sqrt{2})$, $\sigma(\sqrt{2}) = \sqrt{2}$ and $\mathbb{Q}(\sqrt{2}), \sigma(\sqrt{2}) = -\sqrt{2}$ are not isomorphic.*

Example 3.14. *Let k be a σ-field. The σ-m-variety X given by $\sigma(y) \in k\{y\}$, i.e. $X(B) = \mathbb{V}_B(\sigma(y)) = \{b \in B \mid \sigma(b) = 0\}$ for all $B \in \sigma\text{-}\mathbf{int}_k$, has a single point in any σ-field extension of k, namely 0. However, in general integral σ-rings, this is not necessarily the case: Take, for example, $B := k\{y\}/[\sigma(y)] \in \sigma\text{-}\mathbf{int}_k$. In B we have $0 \neq ker(\sigma) = [y + [\sigma(y)]] \trianglelefteq_\sigma B$, which means that in particular, $[y + [\sigma(y)]] \subseteq \mathbb{V}_B(\sigma(y))$.*

It is not a coincidence that in the previous example we found more solutions on the σ-ring $B = k\{y\}/[\sigma(y)]$. The σ-ideal $[\sigma(y)]$ is radical and mixed, i.e. $[\sigma(y)] = \{[\sigma(y)]\}_m$. In fact, the ring B, as we chose it, plays an analogous role to that of the coordinate ring of an affine variety in the usual (algebraic) case.

The next proposition shows why our definition of σ-m-variety is "the right one" for mixed ideals:

Proposition 3.15. *Let k be a σ-field and $X = \mathbb{V}(F) \subseteq \mathbb{A}^n$ be a mixed difference variety over k. Then $\mathbb{I}_m(X) = \{F\}_m \trianglelefteq_\sigma k\{y_1, \ldots, y_n\}$.*

Proof. We will first show that $\mathbb{I}_m(X)$ is a radical, mixed σ-ideal. Let $f,\ g \in \mathbb{I}_m(X)$, $h \in k\{y_1, \ldots, y_n\}$. Then, for every $B \in \sigma\text{-}\mathbf{int}_k$, $b \in \mathbb{V}_B(F)$, we have $f(b) = g(b) = 0$. It follows that $(f + g)(b) = f(b) + g(b) = 0$ as well as $(fh)(b) = f(b)h(b) = 0 \cdot h(b) = 0$ and $\sigma(f)(b) = \sigma(f(b)) = \sigma(0) = 0$, so

that $\mathbb{I}_m(X)$ is a σ-ideal. It further follows that $h(b)^n = 0$ implies $h(b) = 0$, since B is an integral domain, and this means that $h^n \in \mathbb{I}_m(X)$ implies that $h \in \mathbb{I}_m(X)$.

It only remains to show that $\mathbb{I}_m(X)$ is mixed. Let now $f, g \in k\{y_1, \dots, y_n\}$ be such that $fg \in \mathbb{I}_m(X)$. This means that for all $B \in \sigma\text{-}\mathbf{int}_k$, $b \in \mathbb{V}_B(F)$ we have $(fg)(b) = f(b)g(b) = 0$. Since B is an integral domain, this implies that $f(b) = 0$ or $g(b) = 0$. This also implies that $\sigma(f(b)) = \sigma(0) = 0$, or $\sigma(g(b)) = 0$, so that in any case $(f\sigma(g))(b) = 0$, from which it follows that $f\sigma(g) \in \mathbb{I}_m(X)$. We thus see that $\mathbb{I}_m(X)$ is radical and mixed, hence $\{F\}_m \subseteq \mathbb{I}_m(X)$.

For the other inclusion, let $f \in \mathbb{I}_m(X)$. We will show that $f \in \{F\}_m$. Let $F \subseteq \mathfrak{p} \trianglelefteq_\sigma k\{y_1, \dots, y_n\}$ be a prime σ-ideal. Then, consider $B := k\{y_1, \dots, y_n\}/\mathfrak{p}$. This is an integral σ-ring. Since $F \subseteq \mathfrak{p}$, we know that $y + \mathfrak{p} \in \mathbb{V}_B(F)$. By assumption, we have $f \in \mathbb{I}_m(\mathbb{V}(F))$, which means by definition that $f(y + \mathfrak{p}) = 0$, which in turn means that $f \in \mathfrak{p}$. Since this holds for any prime $\mathfrak{p} \trianglelefteq_\sigma R$, Theorem 2.18 implies that $f \in \{F\}_m$. □

Note that, in the notation of the proof above, it does not always have to be the same case, $f(b) = 0$ or $g(b) = 0$, as it depends on B (and b, of course). In particular, $\mathbb{I}_m(X)$ does not have to be prime in general.

From this, we immediately get a further result on radical, mixed ideals, which is analogous to the case of radical ideals in algebraic geometry.

Corollary 3.16. *Let $\mathfrak{a}, \mathfrak{b} \trianglelefteq_\sigma k\{y\}$ be two radical, mixed difference ideals. Then $\mathfrak{a} \cap \mathfrak{b} = \{\mathfrak{a}\mathfrak{b}\}_m$.*

Proof. We can assume that $\mathfrak{a}, \mathfrak{b} \neq \{0\}$, as the assertion is obvious otherwise. Since $\mathfrak{a}, \mathfrak{b}$ are radical and mixed, we know from Proposition 3.15 that $\mathfrak{a} = \mathbb{I}_m(\mathbb{V}(\mathfrak{a}))$, $\mathfrak{b} = \mathbb{I}_m(\mathbb{V}(\mathfrak{b}))$, and $\{\mathfrak{a}\mathfrak{b}\}_m = \mathbb{I}_m(\mathbb{V}(\mathfrak{a}\mathfrak{b}))$. For any $B \in \sigma\text{-}\mathbf{int}_k$, we have:

$$\mathbb{V}_B(\mathfrak{a}\mathfrak{b}) = \mathbb{V}_B(\mathfrak{a}) \cup \mathbb{V}_B(\mathfrak{b}).$$

The inclusion "$\supseteq$" is obvious. For "$\subseteq$", let $p \in \mathbb{V}_B(\mathfrak{a}\mathfrak{b})$ and assume there exists an $f \in \mathfrak{a}$, such that $f(p) \neq 0$. Then, from the definition of $\mathbb{V}_B(\mathfrak{a}\mathfrak{b})$ it follows that $f(p)g(p) = 0$ for all $g \in \mathfrak{b}$. This means, however, that $p \in \mathbb{V}_B(\mathfrak{b})$ (since B is an integral domain). The other case is completely analogous. Since this is true for any B, the σ-m-varieties are also equal: $\mathbb{V}(\mathfrak{a}\mathfrak{b}) = \mathbb{V}(\mathfrak{a}) \cup \mathbb{V}(\mathfrak{b})$. Now,

$$\mathbb{I}_m(\mathbb{V}(\mathfrak{a}\mathfrak{b})) = \mathbb{I}_m(\mathbb{V}(\mathfrak{a}) \cup \mathbb{V}(\mathfrak{b}))$$
$$= \{f \in k\{y\} \mid f(p) = 0 \text{ for all } p \in \mathbb{V}_B(\mathfrak{a}) \cup \mathbb{V}_B(\mathfrak{b}),\ B \in \sigma\text{-}\mathbf{int}_k\},$$

and $f(p) = 0$ for all $p \in \mathbb{V}_B(\mathfrak{a}) \cup \mathbb{V}_B(\mathfrak{b}),\ B \in \sigma\text{-}\mathbf{int}_k$, is equivalent to

$$\underbrace{f(p) = 0 \text{ for all } p \in \mathbb{V}_B(\mathfrak{a}),\ B \in \sigma\text{-}\mathbf{int}_k}_{\Leftrightarrow f \in \mathbb{I}_m(\mathbb{V}(\mathfrak{a}))} \text{ and}$$
$$\underbrace{f(p) = 0 \text{ for all } p \in \mathbb{V}_B(\mathfrak{b}),\ B \in \sigma\text{-}\mathbf{int}_k}_{\Leftrightarrow f \in \mathbb{I}_m(\mathbb{V}(\mathfrak{b}))}.$$

Hence, $\{\mathfrak{a}\mathfrak{b}\}_m = \mathbb{I}_m(\mathbb{V}(\mathfrak{a}\mathfrak{b})) = \mathbb{I}_m(\mathbb{V}(\mathfrak{a})) \cap \mathbb{I}_m(\mathbb{V}(\mathfrak{b})) = \{\mathfrak{a}\}_m \cap \{\mathfrak{b}\}_m = \mathfrak{a} \cap \mathfrak{b}$. □

Definition 3.17. *Let k be a σ-field and let X be a σ-m-variety over k. Further let $F \subseteq k\{y_1, \ldots, y_n\}$ be a system of difference equations over k with $X(B) = \mathbb{V}_B(F)$ for all $B \in \sigma\text{-}\mathbf{int}_k$. Then we consider the σ-ring*

$$k\{y_1, \ldots, y_n\}/\{F\}_m = k\{y_1, \ldots, y_n\}/\mathbb{I}_m(X) =: k\{X\}$$

and call it the coordinate ring *of X. Since $\{F\}_m$ is a radical, mixed σ-ideal, $k\{X\}$ is reduced and well-mixed.*

Remark 3.18. Let k be a σ-field and X a k-σ-m-variety. Further let $b \in X(B),\ B \in \sigma\text{-}\mathbf{int}_k, f + \mathbb{I}_m(X) \in k\{X\}$. Then the value of $f(b) \in k$ is independent of the representative f, since for $f' + \mathbb{I}_m(X) = f + \mathbb{I}_m(X)$, we know that $f - f' \in \mathbb{I}_m(X)$, and thus by definition, $(f - f')(b) = 0$. By abuse of notation, we will sometimes use the representative f to refer to its equivalence class $f + \mathbb{I}_m(X)$ and we will simply write $f(b)$ to mean the well-defined value of evaluating b on any representative of the class.

We can now clarify what we meant after Definition 3.10.

Lemma 3.19. *Let k be a σ-field. Then the maps $X \mapsto \mathbb{I}_m(X)$ and $\mathfrak{a} \mapsto \mathbb{V}(\mathfrak{a})$ define inclusion-reversing bijections between the set of all σ-m-subvarieties of $\mathbb{A}^n$ and the radical, mixed σ-ideals of $k\{y_1, \ldots, y_n\}$.*

Proof. From Proposition 3.15 we know that $\mathbb{I}_m(\mathbb{V}(\mathfrak{a})) = \mathfrak{a}$ is true for all $\mathfrak{a} \trianglelefteq_\sigma k\{y_1, \ldots, y_n\}$ radical, mixed. Conversely, let $X = \mathbb{V}(F) \subseteq \mathbb{A}^n$ be a σ-m-variety. Then we know $\mathbb{V}(\mathbb{I}_m(X)) = \mathbb{V}(\mathbb{I}_m(\mathbb{V}(F))) \subseteq \mathbb{V}(F) = X$, since $F \subseteq \mathbb{I}_m(X)$. On the other hand, it is clear from the definitions of $\mathbb{V}$ and $\mathbb{I}_m$ that $X \subseteq \mathbb{V}(\mathbb{I}_m(X))$, so that $X = \mathbb{V}(\mathbb{I}_m(X))$. This proves the bijectivity of both mappings. That both mappings are inclusion-reversing follows directly from the definitions. □

Note that since every σ-m-variety is a σ-m-subvariety of $\mathbb{A}^n$ for an $n \in \mathbb{N}_{\geq 1}$, it is no restriction to consider $\mathbb{A}^n$ instead of an arbitrary σ-m-variety, as we can see in the following corollary:

Corollary 3.20. *Let X be a σ-m-variety over the σ-field k. Then there is a bijection between the radical, mixed σ-ideals of $k\{X\}$ and the σ-m-subvarieties of X via*

$$X \supseteq Y \mapsto \{f \in k\{X\} \mid f(b) = 0 \text{ for all } b \in Y(B), \text{ for all } B \in \sigma\text{-}\mathbf{int}_k\} =: \mathbb{I}_{k\{X\}}(Y).$$

Proof. If we identify the radical, mixed σ-ideals of $k\{X\}$ with the radical, mixed σ-ideals of $k\{y\}$ which contain $\mathbb{I}_m(X)$ (see Proposition 2.5), then this is just the restriction of the mapping described in Lemma 3.19. □

A further very interesting bijection can also help us to better understand equivalence classes of solutions:

Proposition 3.21. *Let $X = \mathbb{V}(F)$ be a σ-m-variety over the σ-field k. The equivalence classes of solutions of F are in bijection with the σ-m-spectrum of the coordinate ring* $\mathrm{Spec}_m^\sigma(k\{X\})$.

Proof. Let $B \in \sigma\text{-}\mathbf{int}_k$, $b \in B^n$ be a solution of $F \subseteq k\{y_1, \ldots, y_n\}$, i.e. $f(b) = 0$ for all $f \in F$. Consider the mapping

$$\varphi : k\{y_1, \ldots, y_n\} \to B, y \mapsto b.$$

Then $F \subseteq \ker(\varphi) \trianglelefteq_\sigma R$. Since (forgetting the difference structure for a moment), B is an integral domain, the ideal $\ker(\varphi)$ has to be prime. It follows from this that $\{F\}_m = \mathbb{I}_m(X) \subseteq \ker(\varphi)$. In particular, this implies that the mapping φ factors over $\mathbb{I}_m(X)$, and it induces a morphism of σ-rings $\tilde{\varphi} : k\{X\} \to B$. By the same argument as above, the kernel of this induced morphism, $\mathfrak{p}_b :=\ker(\tilde{\varphi}) \trianglelefteq_\sigma k\{X\}$ is a prime σ-ideal of $k\{X\}$. The kernel of the mapping constructed this way is always the same for equivalent solutions. To see this, let $b' \in B'^n$, such that $k\{b\} \cong k\{b'\}$ via $\iota : b \mapsto b'$. Then, for the mapping $\varphi' : k\{y_1, \ldots, y_n\} \to B', y \mapsto b$, we get that $\varphi' = \iota \circ \varphi$ (which is well-defined, since $\mathrm{Im}(\varphi) \subseteq k\{b\}$). In particular, since ι is an isomorphism, $\ker(\varphi) =\ker(\varphi')$. We define the mapping Ψ from the equivalence classes of solutions of F to $\mathrm{Spec}_m^\sigma(k\{X\})$, via $b \mapsto \mathfrak{p}_b$.

On the other hand, for $\mathfrak{p} \in \mathrm{Spec}_m^\sigma(k\{X\})$, which we identify with $\mathbb{I}_m(X) \subseteq \tilde{\mathfrak{p}} \in \mathrm{Spec}_m^\sigma(k\{y_1, \ldots, y_n\})$ (see Proposition 2.5), consider the integral σ-ring $B(\mathfrak{p}) := k\{y_1, \ldots, y_n\}/\tilde{\mathfrak{p}}$. Since $\tilde{\mathfrak{p}}$ is a prime σ-ideal, $B(\mathfrak{p})$ is an integral σ-ring. Set $b(\mathfrak{p}) := \bar{y} \in B(\mathfrak{p})$, as the image of y in $B(\mathfrak{p})$. Then, because $F \subseteq \mathbb{I}_m(X) \subseteq \tilde{\mathfrak{p}}$, we know that $b(\mathfrak{p})$ is a solution of F. We define $\Psi^{-1}(\mathfrak{p})$ as the equivalence class of $b(\mathfrak{p})$. Then Ψ and Ψ^{-1} are inverses of each other, and hence, are both bijections. □

From Proposition 3.21 we see that it is a good idea to concentrate on $\mathrm{Spec}_m^\sigma(k\{X\})$ for a σ-m-variety X over a σ-field k. From here on, we will speak of the "topology on/of X" to refer to the topology on $\mathrm{Spec}_m^\sigma(k\{X\})$, as in Definition 2.24. We will also use the notation $x \in X$ to mean $x \in \mathrm{Spec}_m^\sigma(k\{X\})$, or $T \subseteq X$ closed to speak of a closed subset of $\mathrm{Spec}_m^\sigma(k\{X\})$, and so forth.

3.2 Morphisms of Mixed Difference Varieties

So far we have only studied mixed difference varieties themselves, but not a way to relate them with each other; we have yet to properly define the category of mixed difference varieties over a fixed σ-field k. We still have to define what the morphisms in this category shall be.

Definition 3.22. *Let k be a σ-field, $X \subseteq \mathbb{A}^n, Y \subseteq \mathbb{A}^m$ σ-m-varieties over k. Then, a morphism of functors $f : X \to Y$ is called a* morphism of σ-m-varieties over k *or a* σ-polynomial map*, if there exist σ-polynomials $f_1, \ldots, f_m \in k\{y_1, \ldots, y_n\}$, such that $f(b) = (f_1(b), \ldots, f_m(b))$ for all $b \in X(B), B \in \sigma\text{-}\mathbf{int}_k$.*

Example 3.23. *For two σ-m-varieties $X \subseteq Y = \mathbb{A}_k^n$, over the σ-field k, the inclusion mapping $\iota : X \hookrightarrow Y$ is a morphism of σ-m-varieties over k, since we can choose $f_1 = y_1, f_2 = y_2, \ldots, f_n = y_n$. Similarly, for $m \geq n$ and $X \subseteq \mathbb{A}_k^m, Y \subseteq \mathbb{A}_k^n$ the "projection onto $\mathbb{A}^n$" is also a morphism of σ-m-varieties over k (with the same choice of f_i as the example above).*

Remark 3.24. Let $f : X \to Y$ be a morphism of σ-m-varieties over the σ-field k, $X \subseteq \mathbb{A}^n, Y \subseteq \mathbb{A}^m$. Then, by definition, there exist difference polynomials $f_1, \ldots, f_m \in k\{y_1, \ldots, y_n\}$, such that $f(b) = (f_1(b), \ldots, f_m(b))$ for all $b \in B$, $B \in \sigma\text{-}\mathbf{int}_k$. Modulo $\mathbb{I}_m(X)$, these f_i are unique: If there is $f_1', \ldots, f_m' \in k\{y_1, \ldots, y_n\}$ such that $f_i(b) = f_i'(b)$ for all $b \in B$, $B \in \sigma\text{-}\mathbf{int}_k$, and for all $i \in \underline{m}$, then it follows that $(f_i - f_i')(b) = 0$ for all $b \in B$, $B \in \sigma\text{-}\mathbf{int}_k$, which implies that $f_i - f_i' \in \mathbb{I}_m(X)$ by definition, for all $i \in \underline{m}$.

Now, consider the mapping

$$\phi : k\{z_1, \ldots, z_m\} \to k\{X\},\ z_i \mapsto f_i + \mathbb{I}_m(X) =: \overline{f_i}.$$

This mapping factors over $\mathbb{I}_m(Y)$, since for $h \in \mathbb{I}_m(Y) \subseteq k\{z_1, \ldots, z_m\}$, $b \in X(B)$, $B \in \sigma\text{-}\mathbf{int}_k$, we have that

$$(\phi(h))(b) = h(\overline{f}_1(b), \ldots, \overline{f}_m(b)) = h(f(b)).$$

Since ϕ is a morphism of σ-m-varieties over k, it follows that $f(b) \in Y(B)$, which implies that $h(f(b)) = 0$, by choice of h, hence $h \in \ker(\phi)$. Altogether, this yields a mapping

$$f^* : k\{Y\} \to k\{X\},\ z_i + \mathbb{I}_m(Y) \mapsto y_i + \mathbb{I}_m(X).$$

This mapping is a morphism of integral σ-rings over k, and is called the *dual mapping* or *dual morphism* to f. We have

$$f^*(h)(b) = h(f(b)) \text{ for all } h \in k\{Y\}, b \in X(B),\ B \in \sigma\text{-}\mathbf{int}_k.$$

From the definition it follows that for morphisms $X \xrightarrow{f} Y \xrightarrow{g} Z$ of σ-m-varieties over k, we get $(f \circ g)^* = g^* \circ f^*$. We thus get a contravariant functor $-^*$ from the category of mixed difference varieties over k to $\sigma\text{-}\mathbf{ring}_k$.

Proposition 3.25. *Let k be a σ-field. Then $-^*$, as defined in Remark 3.24, is an anti-equivalence between the category of σ-m-varieties over k and the subcategory of $\sigma\text{-}\mathbf{ring}_k$, which arises by restricting the object class to reduced, well-mixed, finitely σ-generated σ-overrings of k. In particular, a morphism $f : X \to Y$ of σ-m-varieties over k is an isomorphism if and only if $f^* : k\{Y\} \to k\{X\}$ is an isomorphism.*

Proof. Since for a σ-m-variety X over k, $\mathbb{I}_m(X)$ is radical and mixed, $k\{X\}$ is always a reduced and well-mixed σ-overring of k, and finitely σ-generated since σ-m-varieties are defined only for equations with finitely many difference variables. From this it follows that the functor $-^*$ from Remark 3.24 is well defined.

It suffices to show that it is surjective on the skeleton of the categories and bijective on morphisms. Let B be a finitely σ-generated, well-mixed and reduced σ-overring of k. We can then write $B \cong k\{y_1, \ldots, y_n\}/\mathfrak{a}$, for an $\mathfrak{a} \trianglelefteq_\sigma k\{y_1, \ldots, y_n\}$ radical and mixed. The σ-m-variety $X = \mathbb{V}(\mathfrak{a}) \subseteq \mathbb{A}^n$ is then a preimage of the isomorphism class of B, since $\mathbb{I}_m(X) = \mathbb{I}_m(\mathbb{V}(\mathfrak{a})) = \mathfrak{a}$, because of Proposition 3.15. Thus, $B \cong k\{X\}$.

Now, for the morphisms: First, let X, Y be σ-m-varieties over k and $f, g \in \mathrm{Hom}(X, Y)$ with $f^* = g^*$. Then we know that for every $h \in k\{X\}$, and every $b \in B,\ B \in \sigma\text{-}\mathbf{int}_k$:

$$h(f(b)) = (f^*(h))(b) = (g^*(h))(b) = h(g(b)).$$

In particular, $f(b) = g(b)$ for all $b \in B,\ B \in \sigma\text{-}\mathbf{int}_k$, which implies that $f = g$, and $-^*$ is injective. On the other hand, let $\varphi : k\{Y\} \to k\{X\}$ be a morphism of σ-overrings of k. There exist $n, m \in \mathbb{N}_{\geq 1}$ such that $X \subseteq \mathbb{A}^n, Y \subseteq \mathbb{A}^m$, which means that $k\{X\} = k\{z_1, \ldots, z_n\}/\mathbb{I}_m(X)$ and

$k\{Y\} = k\{y_1, \ldots, y_m\}/\mathbb{I}_m(Y)$. We will construct a preimage of φ: Choose $f_1, \ldots, f_m \in k\{z_1, \ldots, z_n\}$ such that $\varphi(y_i + \mathbb{I}_m(Y)) = f_i + \mathbb{I}_m(X)$ for all $i \in \underline{m}$. Then we define a morphism $f : X \to Y$ of σ-m-varieties over k as follows: $f(b) := (f_1(b), \ldots, f_m(b))$ for all $b \in B,\ B \in \sigma\textbf{-int}_k$. This is well-defined: Let $h \in \mathbb{I}_m(Y)$. Then, by definition, $h(y_1 + \mathbb{I}_m(Y), \ldots, y_n + \mathbb{I}_m(Y)) = 0 + \mathbb{I}_m(Y)$. This implies that $h(f_1 + \mathbb{I}_m(X), \ldots, f_m + \mathbb{I}_m(X)) = 0 + \mathbb{I}_m(X)$, since φ is a morphism of σ-overrings of k. This in turn implies that $h(f(b)) = 0$ for all $b \in X(B),\ B \in \sigma\textbf{-int}_k$, which means that f indeed maps onto Y and $f^* = \varphi$, by construction. □

This gives us a pretty good idea about the importance of the coordinate ring in difference algebra. Having defined a category for σ-m-varieties, we can now see how this new category-theoretic language helps us to better understand the topological aspects of mixed difference varieties.

Lemma 3.26. *Let R, S, T be σ-rings, and $\varphi : R \to S,\ \psi : S \to T$ morphisms of σ-rings. Then the mapping*

$$\tilde{\varphi} : \operatorname{Spec}_m^\sigma(S) \to \operatorname{Spec}_m^\sigma(R), \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$$

induced by φ is continuous. In fact, we have $\widetilde{\psi \circ \varphi} = \tilde{\varphi} \circ \tilde{\psi}$, and in particular, $R \mapsto \operatorname{Spec}_m^\sigma(R)$ with $\psi \mapsto \tilde{\psi}$ is a contravariant functor from the category of σ-rings to **Top**, *the category of topological spaces.*

Proof. Let $A = \mathcal{V}_m(F) \subseteq \operatorname{Spec}_m^\sigma(R)$ be closed. We have to show that $\tilde{\varphi}^{-1}(A) \subseteq \operatorname{Spec}_m^\sigma(S)$ is closed. We have,

$$\begin{aligned}\tilde{\varphi}^{-1}(A) = \tilde{\varphi}^{-1}(\mathcal{V}_m(F)) &= \{\mathfrak{p} \in \operatorname{Spec}_m^\sigma(S) \mid F \subseteq \varphi^{-1}(\mathfrak{p})\} \\ &= \{\mathfrak{p} \in \operatorname{Spec}_m^\sigma(S) \mid \varphi(F) \subseteq \mathfrak{p}\} = \mathcal{V}_m(\varphi(F)).\end{aligned}$$

The equality $\widetilde{\psi \circ \varphi} = \tilde{\varphi} \circ \tilde{\psi}$ is immediately clear from the definitions. □

We thus see how radical, mixed σ-ideals and the definition of σ-m-varieties as functors from $\sigma\textbf{-int}_k$, for a σ-field k, as well as the topology defined on $\operatorname{Spec}_m^\sigma(k\{X\})$ all fit together. These are all in analogous relations to the case for perfect σ-ideals and the Cohn topology outlined in Section 1. We will try to shed some light on the choice of the category $\sigma\textbf{-int}_k$ here:

Definition 3.27. *Let k be a σ-field.*

(a) We denote by $\sigma\textbf{-VarField}_k$ the category of σ-varieties (as defined in Section 1). It has functors of the form $B \mapsto \mathbb{V}_B(F)$ as objects, where B is a σ-field extension of k. As morphisms it has σ-polynomial maps defined in a fashion analogous to Definition 3.22.

(b) *Similarly, we denote by* σ-$\mathbf{VarDomain}_k$ *the category which has functors of the form* $B \mapsto \mathbb{V}_B(F)$ *as objects, where* B *is a* σ*-domain extension of* k*, and as morphisms* σ*-polynomial maps defined in a fashion analogous to Definition 3.22. We define* $\mathbb{I}_{\mathrm{Domain}}(X)$ *for* $X \in \sigma$-$\mathbf{VarDomain}_k$ *and* $\mathbb{V}_{\mathrm{Domain}}(F)$ *analogous to Definitions 3.5 and 3.8.*

(c) *Finally, we denote by* σ-$\mathbf{VarRing}_k$ *the category which has functors of the form* $B \mapsto \mathbb{V}_B(F)$ *as objects, where* $B \supseteq k$ *is a perfectly* σ*-reduced ring over* k*, and as morphisms* σ*-polynomial maps defined in a fashion analogous to Definition 3.22. We also define* $\mathbb{I}_{\mathrm{Ring}}(X)$ *for* $X \in \sigma$-$\mathbf{VarRing}_k$ *and* $\mathbb{V}_{\mathrm{Ring}}(F)$ *analogous to Definitions 3.5 and 3.8.*

In all three cases $F \subseteq k\{y\}$ *denotes a set of* σ*-polynomials on finitely many difference variables* $y = (y_1, \ldots, y_n)$*.*

Proposition 3.28. *Let* k *be a* σ*-field. The three categories* σ-$\mathbf{VarField}_k$*,* σ-$\mathbf{VarDomain}_k$ *and* σ-$\mathbf{VarRing}_k$ *are equivalent.*

Proof. Similar to Proposition 3.25, the category of σ-varieties σ-$\mathbf{VarField}_k$ is anti-equivalent to the category of perfectly σ-reduced σ-overrings of k which are finitely σ-generated over k (see [1], Theorem 2.1.21). It suffices to show that the other two categories are also anti-equivalent to it. From the proof of Proposition 3.25 we can see that it is enough to show that $\mathbb{I}_{\mathrm{Domain}}(\mathbb{V}_{\mathrm{Domain}}(\mathfrak{a})) = \{\mathfrak{a}\}$, and $\mathbb{I}_{\mathrm{Ring}}(\mathbb{V}_{\mathrm{Ring}}(\mathfrak{a})) = \{\mathfrak{a}\}$, where $\mathfrak{a} \trianglelefteq_\sigma k\{y\}$ is a σ-ideal and $\{\mathfrak{a}\}$ its perfect closure.

Let first $X = \mathbb{V}_{\mathrm{Ring}}(F) \in \sigma$-$\mathbf{VarRing}_k$ be a σ-variety in this sense of perfectly reduced σ-rings. We first show that

$$\mathbb{I}_{\mathrm{Ring}}(X) = \{f \in k\{y\} \mid f(b) = 0 \text{ for all } b \in \mathbb{V}_B(F), \\ B \supseteq k \text{ perfectly } \sigma\text{-reduced}\}$$

is a perfect σ-ideal. Similar to Proposition 3.15, we know that $\mathbb{I}_{\mathrm{Ring}}(X)$ is a difference ideal. Let $f \in k\{y\}$ with $\sigma^{i_1}(f) \cdots \sigma^{i_r}(f) \in \mathbb{I}_{\mathrm{Ring}}(X)$. This means that for all $b \in \mathbb{V}_B(F)$, B perfectly σ-reduced: $\sigma^{i_1}(f)(b) \cdots \sigma^{i_r}(f)(b) = 0$. Since B is perfectly σ-reduced, this means that $f(b) = 0$ for all such b, which in turn, by definition, means that $f \in \mathbb{I}_{\mathrm{Ring}}(X)$. Since every σ-domain is perfectly σ-reduced, the argument also works for $X \in \sigma$-$\mathbf{VarDomain}_k$, with $\mathbb{I}_{\mathrm{Domain}}$ instead of $\mathbb{I}_{\mathrm{Ring}}$. This implies that

$$\{F\} \subseteq \mathbb{I}_{\mathrm{Domain}}(\mathbb{V}_{\mathrm{Domain}}(F)), \text{ as well as } \{F\} \subseteq \mathbb{I}_{\mathrm{Ring}}(\mathbb{V}_{\mathrm{Ring}}(F)).$$

For the other inclusion "$\supseteq$", we shall first consider $X \in \sigma$-$\mathbf{VarDomain}_k$. For $F \subseteq k\{y\}$, we have $\{F\} \supseteq \mathbb{I}_{\mathrm{Domain}}(\mathbb{V}_{\mathrm{Domain}}(F))$. To show this, let

$f \in \mathbb{I}_{\text{Domain}}(\mathbb{V}_{\text{Domain}}(F))$. We know that $\{F\}$ is the intersection of all σ-prime ideals of $k\{y\}$ which contain F (see Theorem 1.18), so it is enough to show that $f \in \mathfrak{p}$ for each σ-prime $\mathfrak{p} \trianglelefteq_\sigma k\{y\}$ with $F \subseteq \mathfrak{p}$. We define the σ-domain $B := k\{y\}/\mathfrak{p} =: k\{a\}$, with $a := y + \mathfrak{p} \in k\{y\}/\mathfrak{p}$. Since $F \subseteq \mathfrak{p}$, we get $a \in \mathbb{V}_B(F)$, which, by definition of $\mathbb{I}_{\text{Domain}}(\mathbb{V}_{\text{Domain}}(F))$, means that $f(a) = 0$. Hence, $f \in \mathfrak{p}$ for all σ-prime $\mathfrak{p}$ with $F \subseteq \mathfrak{p}$, which in turn implies that $f \in \{F\}$. Since every σ-domain B is perfectly σ-reduced, this works for the category σ-$\mathbf{VarRing}_k$ as well, with $\mathbb{I}_{\text{Ring}}, \mathbb{V}_{\text{Ring}}$ instead of $\mathbb{I}_{\text{Domain}}, \mathbb{V}_{\text{Domain}}$. □

While there are many analogies with the Cohn topology, a very important aspect still remains open. Perfect difference ideals of $k\{y\}$ satisfy the ascending chain condition (see Chapter 3, Theorem IV of [5]), which means that the Cohn topology yields a Noetherian topological space. In fact, there is a generalization of the Hilbert basis theorem for this case; see Chapter 3, Theorem V of [5]. The methods used to prove this in [5] do not seem to work as simply for the case of radical, mixed difference ideals. In fact, as far as the author knows, it is still not known if radical, mixed difference ideals satisfy the ascending chain condition. Mixed difference ideals do not satisfy it, as was shown by Levin in [10].

4 Difference Kernels

In this section we will see a further approach to investigating difference ideals. We will study the properties of difference ideals of difference polynomial rings by looking at its intersections with the variables up to a finite power of sigma.

4.1 Difference Kernels

Definition 4.1. *Let k be a difference field and $d \in \mathbb{N}$. Then we define $k\{y\}[d] := k[y, \sigma(y), \ldots, \sigma^d(y)] \subseteq k\{y\}$ and we set $k\{y\}[-1] := k$. Let $\mathfrak{a} \trianglelefteq_\sigma k\{y\}$ be a difference ideal in the σ-polynomial ring $k\{y\}$. We set $\mathfrak{a}[d] := \mathfrak{a} \cap k\{y\}[d]$.*

Definition 4.2. *Let $\mathfrak{a} \trianglelefteq k\{y\}[d], d \geq 1$ be an ideal of $k\{y\}[d]$. Then $\mathfrak{a}$ is called a* difference kernel of length d, *if $\sigma(\mathfrak{a}[d-1]) \subseteq \mathfrak{a}$. The difference kernel is called* prime, *if additionally $\mathfrak{a}$ is a prime ideal of $k\{y\}[d]$. Finally, $\mathfrak{a}$ is called a* reflexive difference kernel of length d, *if $\sigma^{-1}(\mathfrak{a}) = \mathfrak{a}[d-1]$.*

It is worth noting that this notation differs from that of the standard literature (in particular [5] and [6]). In the standard literature, the quotient ring obtained by factoring out what was defined here as a prime, reflexive kernel is called a kernel. The rest of the concepts are not treated. We chose to change the notation to be able to study other σ-ideals with this methodology.

Remark 4.3. Clearly, a reflexive kernel is always a kernel, but the converse is not necessarily true. That $\mathfrak{a}$ is a kernel of length d only guarantees the inclusion $\mathfrak{a}[d-1] \subseteq \sigma^{-1}(\mathfrak{a})$.

Example 4.4. *Let $\mathfrak{p} \trianglelefteq_\sigma k\{y\}$ be a prime σ-ideal, $d \geq 1$. Then $\mathfrak{p}[d] \trianglelefteq k\{y\}[d]$ is a prime kernel. Since $\mathfrak{p}$ is a σ-ideal we have $\sigma(\mathfrak{p}[d-1]) \subseteq \mathfrak{p}$, and since $\mathfrak{p}$ is prime, we know that $\mathfrak{p}[d]$ has to be prime as well. If $\mathfrak{p}$ is also reflexive (i.e. a σ-prime ideal), then $\mathfrak{p}[d]$ is a reflexive, prime kernel.*

Inspired by the previous example we define the following:

Definition 4.5. *Let $\mathfrak{a} \trianglelefteq k\{y\}[d]$ be a kernel of length d, and $\mathfrak{a}' \trianglelefteq_\sigma k\{y\}$ be a σ-ideal. Then we call $\mathfrak{a}'$ a* realization *of $\mathfrak{a}$, if $\mathfrak{a} \subseteq \mathfrak{a}'$, and we call the realization* regular, *if in addition $\mathfrak{a}'[d] = \mathfrak{a}$. Similarly, if $\mathfrak{a}$ is a reflexive(prime) kernel, then we define a realization to be a* reflexive(prime) realization, *if the σ-ideal $\mathfrak{a}'$ is reflexive/prime.*

The former example and the accompanying definition are actually much more general than it would seem at first sight. It is in fact the case that

prime, reflexive kernels are always of the form $\mathfrak{p}[d]$ for a σ-prime ideal $\mathfrak{p}$ (this is the content of the upcoming Theorem 4.10). For prime kernels which are not necessarily reflexive this is not as simple, as we will later see.

Remark 4.6. Let $\mathfrak{p} \subseteq k\{y\}[d]$ be a difference kernel of length d. Then, σ induces a well-defined mapping

$$\sigma : k[y, \ldots, \sigma^{d-1}(y)]/\mathfrak{p}[d-1] \to k[y, \ldots, \sigma^{d}(y)]/\mathfrak{p}$$

If $\mathfrak{p}$ is a reflexive kernel, then this mapping is injective. We set $a := \bar{y} = y + \mathfrak{p} \in k\{y\}[d]/\mathfrak{p}$. If $\mathfrak{p}$ is a prime, reflexive kernel, then we can extend σ to the quotient fields:

$$\begin{aligned}\sigma : k(a, \ldots, \sigma^{d-1}(a)) \cong \operatorname{Quot}(k[y, \ldots, \sigma^{d-1}(y)]/\mathfrak{p}[d-1]) \\ \to k(a, \ldots, \sigma^{d}(a)) = k(\mathfrak{p}).\end{aligned}$$

Even in the general case of prime difference kernels we can work with the properties of field extensions, though we cannot properly extend σ to the fields. In particular, we get a nice way of defining some sort of "difference degree" of prime kernels:

Definition 4.7. *Let $\mathfrak{p} \subseteq k\{y\}[d]$ be a prime difference kernel of length d, and let $a := y + \mathfrak{p} \in k(\mathfrak{p})$. We define the difference dimension of $\mathfrak{p}$ as follows:*

$$\begin{aligned}\sigma\text{-dim}(\mathfrak{p}) &:= \operatorname{trdeg}(k(\mathfrak{p})/k(\mathfrak{p}[d-1]) \\ &= \operatorname{trdeg}(\operatorname{Quot}((k\{y\}[d]/\mathfrak{p}))/\operatorname{Quot}(k\{y\}[d-1]/\mathfrak{p}[d-1])) \\ &= \operatorname{trdeg}(k(a, \ldots, \sigma^{d}(a))/k(a, \ldots, \sigma^{d-1}(a))).\end{aligned}$$

If we want to study prime, reflexive difference kernels as the intersection of σ-prime ideals with $k\{y\}[d]$, it is reasonable to consider some sort of extension, or *prolongation* of a kernel, which would be the intersection with $k\{y\}[d+1]$. This motivates the following definition:

Definition 4.8. *Let $\mathfrak{a} \subseteq k\{y\}[d]$ be a difference kernel of length d, and $\mathfrak{a}' \supset \mathfrak{a}$ be a further difference kernel, of length $d+1$. Then we call $\mathfrak{a}'$ a* prolongation *of $\mathfrak{a}$, if $\mathfrak{a}'[d] = \mathfrak{a}$. Similarly, for a prime(reflexive) kernel we say the prolongation is prime(reflexive), if $\mathfrak{a}'$ is also prime(reflexive). For a prime prolongation, if additionally $\sigma\text{-dim}(\mathfrak{a}) = \sigma\text{-dim}(\mathfrak{a}')$, we call the prolongation* generic.

Definition 4.9. *Let $\mathfrak{p} \subseteq k\{y\}$ be a prime difference kernel of length d, and let $\mathfrak{p}'$ be a regular, prime realization of $\mathfrak{p}$. We call $\mathfrak{p}'$ a* principal realization *of $\mathfrak{p}$, if $\mathfrak{p}'[i+1]$ is a generic prolongation of $\mathfrak{p}'[i]$, for all $i \geq d$.*

As mentioned above, the case of reflexive, prime kernels is well understood. It can be summarized by the following Theorem, which can be found as Corollary 5.2.8 of [1]:

Theorem 4.10. *Let $\mathfrak{q} \subseteq k\{y\}$ be a prime, reflexive kernel of length d. Then there exists a reflexive, principal realization of $\mathfrak{q}$.*

The situation is not as simple for prime kernels that are not necessarily reflexive, as shown by the following example.

Example 4.11. *Consider the difference polynomials $f_1 := \sigma(y_2) + 1, f_2 := \sigma(y_1)y_2 + y_1y_2 + \sigma(y_1) + y_1 + y_2 \in \mathbb{Q}[y_1, y_2, \sigma(y_1), \sigma(y_2)] =: R$. A calculation with [9] quickly identifies that the ideal $(f_1, f_2) \trianglelefteq R$ is prime, and in fact, f_1, f_2 is a Gröbner Basis of (f_1, f_2) with respect to the graded reverse-lexicographical term ordering $y_2 < y_1 < \sigma(y_2) < \sigma(y_1)$. This means that $(f_1, f_2)[0] = \{0\}$, and thus (f_1, f_2) is a prime kernel of length 1 of $\mathbb{Q}\{y_1, y_2\}$. However,*

$$f_1 \cdot (\sigma^2(y_1) + \sigma(y_1) + 1) - \sigma(f_2) = 1,$$

which means that any σ-ideal of $\mathbb{Q}\{y_1, y_2\}$ containing f_1, f_2 is already the whole ring, and is not prime, by definition. The commented code for this example can be found in Appendix A.

As the example shows, prime kernels are not always the intersection of a prime difference ideal with $k\{y\}[d]$. If we want to try and classify those prime kernels that are in fact such intersections, we can try and find necessary conditions to be able to find a prolongation of a kernel. We will develop a condition that is necessary, but not sufficient. First, however, we need a few further results to help prove this.

Lemma 4.12. *Let $R \subseteq S$ be integral domains. Let $I \trianglelefteq R[y]$ be an ideal in the polynomial ring over R in the (not necessarily finite) tuple of variables $y = (y_1, y_2, \ldots)$. Consider the ideal generated by I in $S[y]$, which we will denote by (I). Then*

$$S[y]/(I) \cong (R[y]/I) \otimes_R S.$$

Proof. We consider the following short exact sequence:

$$0 \to I \to R[y] \to R[y]/I \to 0. \tag{3}$$

Since the tensor product is right exact, if we tensor the Sequence (3) over R with S we get the exact sequence

$$I \otimes_R S \xrightarrow{\mathrm{Id}_I \otimes \mathrm{Id}_S} \underbrace{R[y] \otimes_R S}_{\cong S[y]} \xrightarrow{\varphi} (R[y]/I) \otimes_R S \longrightarrow 0.$$

Where $S \otimes_R R[y] \cong S[y]$ follows from the fact that the tuple of variables $y = (y_1, y_2, \ldots)$ is algebraically independent. By the fundamental theorem on homomorphisms we thus get that

$$(R[y]/I) \otimes_R S \cong \underbrace{S \otimes_R R[y]}_{\cong S[y]} / \ker(\varphi).$$

However, since the sequence is exact, we have

$$\begin{aligned}\ker(\varphi) = \mathrm{Im}(\mathrm{Id}_I \otimes \mathrm{Id}_S) &\cong \left\{ \sum_{i=1}^{k} s_i f_i \mid s_i \in S, f_i \in I, k \geq 0 \right\} \\ &= \left\{ \sum_{i=1}^{k} g_i f_i \mid g_i \in S[y], f_i \in I, k \geq 0 \right\} = (I) \trianglelefteq S[y],\end{aligned}$$

from which the statement follows. □

Proposition 4.13. *Let $R \subseteq S$ be integral domains. Let $I \trianglelefteq R[y]$ be an ideal in the polynomial ring over R in n variables and assume that $I \cap R = 0$. Consider the ideal generated by I in $S[y]$, which we will denote by (I). Then $(I) \cap S = 0$.*

Proof. Let $R' := R[y]/I$ and $S' := S[y]/(I)$. Our assumption $R \cap I = 0$ can then be rewritten as the equivalent condition that the mapping

$$R \to R', r \mapsto r + I$$

is injective.

Similarly, we want to show that the analogous mapping $S \to S'$, $s \mapsto s + (I)$ is injective, which is equivalent to the assertion that $(I) \cap S = 0$.

By Lemma 4.12 we have

$$S' = S[y]/(I) \cong R' \otimes_R S.$$

Let $E := \mathrm{Quot}(S)$ and $F := \mathrm{Quot}(R)$ be the fraction fields of the integral domains S and R respectively. Since E is a field, E is a flat F module. Similarly, since F as the fraction field of R is a localization of the former, F is a flat R module (see Theorem 1 in Ch. II § 2.4 of [8]). Together these two facts imply that E is a flat R module as well. To see this, let $J \trianglelefteq R$ be finitely generated (it suffices to consider finitely generated ideals of R, see for example Proposition 6.1 of [3]). Since F is a flat R module, the mapping $J \otimes_R F \hookrightarrow R \otimes_R F \cong F$ is injective. Further, since E is a flat F module, we can tensor this mapping with E over F and get the injective mapping

$$J \otimes_R F \otimes_F E \cong J \otimes_R E \hookrightarrow (R \otimes_R F) \otimes_F E \cong F \otimes_F E \cong E.$$

This is exactly the flatness of E as an R module. We can then conclude that if we take the tensor product over R with E from the mapping $R \to R'$ it will remain injective. This means that the sequence

$$E \otimes_R R \cong E \hookrightarrow E \otimes_R R',\ e \otimes_R r \mapsto e \otimes_R (r + I)$$

is injective. Furthermore, the canonical embedding $S \hookrightarrow E = \mathrm{Quot}(S)$ is also injective. So that we get an injective mapping from the composition:

$$S \hookrightarrow E \otimes_R R', s \mapsto s \otimes_R (1 + I).$$

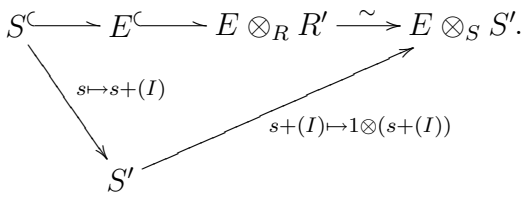
Additionally, we have

$$E \otimes_R R' \cong (E \otimes_S S) \otimes_R R' \cong E \otimes_S \underbrace{(S \otimes_R R')}_{\cong S', \text{ see above}} \cong E \otimes_S S'.$$

The composition of this isomorphism with the mapping above yields the injectivity of the mapping

$$S \hookrightarrow E \otimes_S S', s \mapsto s \otimes_S (1 + (I)) = 1 \otimes_S s(1 + (I)) = 1 \otimes_S (s + (I)).$$

This implies that the following diagram is commutative:



Since the mapping $S \hookrightarrow E \otimes_S S'$ is injective, this means that the mapping $S \to S'$ is injective as well, which is what we wanted to show. □

Lemma 4.14. *Let R be an integral domain and $I \trianglelefteq R[y]$ be an ideal of $R[y] = R[y_1, \ldots, y_n]$, which satisfies $I \cap R = \{0\}$. Then there exists a prime ideal P with $I \subseteq P \subseteq R[y]$, such that $P \cap R = \{0\}$.*

Proof. We can assume without loss of generality that I is radical: Namely, if $f \in \sqrt{I} \cap R$, then there exists an $m \in \mathbb{N}$, such that $f^m \in I \cap R = \{0\}$, and since R is an integral domain this already means that $f = 0$.

We then note that for two sets $A, B \subseteq R[y]$ we have the inclusion $\sqrt{(A)}\sqrt{(B)} \subseteq \sqrt{(AB)}$: Consider $f \in \sqrt{(A)}, g \in \sqrt{(B)}$. Then there exist $m, \tilde{m} \in \mathbb{N}$, such that $f^m \in (A), g^{\tilde{m}} \in (B)$; assume without loss of generality that $m > \tilde{m}$, then $(fg)^m \in (A)(B)$, which implies $fg \in \sqrt{(A)(B)} = \sqrt{(AB)}$. Now, for the proof, consider the set of all radical ideals J containing I, such

that $J \cap R = \{0\}$. This set is not empty and is inductively ordered by inclusion. By Zorn's lemma this means that there exists a maximal element P of this set. This ideal P is prime. To see this, assume there exist $f, g \notin P$ with $fg \in P$. Then the radical ideals $\sqrt{P \cup \{f\}}$, $\sqrt{P \cup \{f\}}$ strictly include P, and by the maximality of P it means there exist $t_1, t_2 \in R \backslash \{0\}$, such that $t_1 \in \sqrt{P \cup \{f\}}$, $t_2 \in \sqrt{P \cup \{g\}}$. In particular, because R is free of zero divisors, this implies that

$$0 \neq t_1 t_2 \in \sqrt{P \cup \{f\}}\sqrt{P \cup \{g\}} \subseteq \underbrace{\sqrt{(P \cup \{f\})(P \cup \{g\})}}_{\subseteq P, \text{ since } fg \in P} = P,$$

a contradiction. □

Proposition 4.15. *Let $\mathfrak{p} \subseteq k\{y\}[d]$ be a reflexive, prime difference kernel of length d. Then $\mathfrak{p}$ has a reflexive, prime prolongation $\mathfrak{p}' \subseteq k\{y\}[d+1]$.*

Proof. See Lemma 5.2.6 of [1]. □

The statement of Proposition 4.15 is an example where the simple generalization fails in our case, namely when the kernel is not necessarily reflexive (as shown by Example 4.11). We can find a condition equivalent to the existence of a prime prolongation for a prime kernel:

Proposition 4.16. *Let $\mathfrak{a} \subseteq k[y, \ldots, \sigma^d(y)]$ be a prime difference kernel of length d and let $k[y, \ldots, \sigma^d(y)]/\mathfrak{a} =: k[a, \sigma(a), \ldots, \sigma^d(a)]$. Consider the mapping*

$$\sigma : k[a, \ldots, \sigma^{d-1}(a)] \to k[a, \ldots, \sigma^d(a)].$$

Then $\mathfrak{a}$ has a prime prolongation, if and only if for the ideal generated by $\ker(\sigma)$*, which we will denote by* $(\ker(\sigma)) \subseteq k[a, \ldots, \sigma^d(a)]$*, we have*

$$(\ker(\sigma)) \cap k[a, \ldots, \sigma^{d-1}(a)] = \ker(\sigma). \tag{4}$$

Proof. First, we assume that Equation (4) holds and will construct a prime prolongation $\mathfrak{a}$.

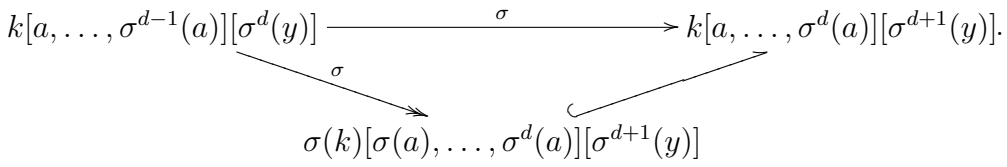
Consider the surjective mapping

$$k[a, \ldots, \sigma^{d-1}(a)][\sigma^d(y)] \to k[a, \ldots, \sigma^d(a)], \sigma^d(y) \mapsto \sigma^d(a).$$

Let $\mathfrak{p}_1$ be the kernel of this mapping. Since $k[a, \ldots, \sigma^d(a)]$ is a domain, we know by the fundamental theorem on homomorphisms that $\mathfrak{p}_1$ has to be prime. First, we will show that our assumption on $\ker(\sigma)$ holds, if and only if:

$$\underbrace{\sigma(\mathfrak{p}_1)}_{\subseteq \sigma(k)[\sigma(a), \ldots, \sigma^d(a)][\sigma^{d+1}(y)]} \cap \sigma(k)[\sigma(a), \ldots, \sigma^d(a)] = 0. \tag{5}$$

To see this consider the following commutative diagram:



We can factor out $\mathfrak{p}_1$ and its image, $\sigma(\mathfrak{p}_1)$. Since

$$k[a,\ldots,\sigma^{d-1}(a)][\sigma^d(y)]/\mathfrak{p}_1 \cong k[a,\ldots,\sigma^d(a)],$$

we get a surjectve mapping

$$k[a,\ldots,\sigma^d(a)] \twoheadrightarrow \sigma(k)[\sigma(a),\ldots,\sigma^d(a)][\sigma^{d+1}(y)]/\sigma(\mathfrak{p}_1).$$

The kernel of this mapping is, by definition of $\mathfrak{p}_1$, $(\ker(\sigma))$. If we factor it out, we get an isomorphism:

$$k[a,\ldots,\sigma^d(a)]/(\ker(\sigma)) \cong \sigma(k)[\sigma(a),\ldots,\sigma^d(a)][\sigma^{d+1}(y)]/\sigma(\mathfrak{p}_1).$$

On the other hand, we have the canonical embedding

$$k[a,\ldots,\sigma^{d-1}(a)] \hookrightarrow k[a,\ldots,\sigma^d(a)].$$

This mapping stays injective after factoring out the kernel of σ on both sides, i.e. $k[a,\ldots,\sigma^{d-1}(a)]/\ker(\sigma) \hookrightarrow k[a,\ldots,\sigma^d(a)]/(\ker(\sigma))$ is injective, if and only if our assumption on $\ker(\sigma)$ holds. In this case, by composition with the isomorphism above, we get an embedding:

$$k[a,\ldots,\sigma^{d-1}(a)]/\ker(\sigma) \hookrightarrow \sigma(k)[\sigma(a),\ldots,\sigma^d(a)][\sigma^{d+1}(y)]/\sigma(\mathfrak{p}_1).$$

This proves Equation (5), since the mapping is injective, if and only if Equation (5) holds. By Proposition 4.13, Equation (5) then implies that

$$(\sigma(\mathfrak{p}_1)) \cap k[a,\sigma(a),\ldots,\sigma^d(a)] = 0. \tag{6}$$

We will now construct a prime difference kernel $\tilde{\mathfrak{a}}$ using Equation (6):

By Lemma 4.14 there exists a prime ideal $\tilde{\mathfrak{p}}_2 \supset (\sigma(\mathfrak{p}_1))$ of the ring $k[a,\ldots,\sigma^d(a)][\sigma^{d+1}(y)]$ containing $\sigma(\mathfrak{p}_1)$ with $\tilde{\mathfrak{p}}_2 \cap k[a,\ldots,\sigma^d(a)] = 0$. Let $\mathfrak{p}_2 \subseteq \tilde{\mathfrak{p}}_2$ be a minimal prime ideal over $(\sigma(\mathfrak{p}_1))$. Since $\mathfrak{p}_2 \subseteq \tilde{\mathfrak{p}}_2$, we have $\mathfrak{p}_2 \cap k[a,\ldots,\sigma^d(a)] = 0$. We thus get a well-defined mapping

$$\sigma : k[a,\ldots,\sigma^{d-1}(a)][\sigma^d(y)]/\mathfrak{p}_1 \to k[a,\ldots,\sigma^d(a)][\sigma^{d+1}(y)]/\mathfrak{p}_2.$$

We define $R_2 := k[a, \ldots, \sigma^d(a)][\sigma^{d+1}(y)]/\mathfrak{p}_2 =: k[a, \ldots, \sigma^d(a), \sigma^{d+1}(a)]$, which is an integral domain since $\mathfrak{p}_2$ is prime. Since $\mathfrak{p}_2 \cap k[a, \ldots, \sigma^d(a)] = 0$ we can use this notation unambiguously: this guarantees namely that for $a, \ldots, \sigma^d(a)$ we have the same residue classes modulo $\mathfrak{p}_2$ as we had modulo $\mathfrak{a}$. The kernel $\tilde{\mathfrak{a}}$ of the natural epimorphism $k[y, \ldots, \sigma^{d+1}(y)] \to R_2$ is thus a prime ideal. Further we have $\mathfrak{a} \subseteq \tilde{\mathfrak{a}}$ by construction (as $\mathfrak{a} = 0 \subset R_2$). In fact, we have $\tilde{\mathfrak{a}}[d] = \mathfrak{a}$ since:

$$\tilde{\mathfrak{a}}[d] = \{f \in k[y, \ldots, \sigma^d(y)] \mid f(a) = 0\} = \ker(k\{y\}[d] \to k[a, \ldots, \sigma^d(a)]) = \mathfrak{a},$$

where the first equality uses the fact that $\mathfrak{p}_2 \cap k[a, \ldots, \sigma^d(a)] = 0$, as noted by the use of the notation explained above, and the last equality holds by definition of $a \in k[a, \ldots, \sigma^d(a)]$. This means that $\tilde{\mathfrak{a}}$ is a prime prolongation of $\mathfrak{a}$.

This proves the direction "$\Leftarrow$". We will now show the other implication. If $\mathfrak{a}$ has a prime prolongation, then by definition there exists a prime difference kernel $\tilde{\mathfrak{a}} \subseteq k[y, \ldots, \sigma^{d+1}(y)]$ of length $d+1$ with $\tilde{\mathfrak{a}} \cap k[y, \ldots, \sigma^d(y)] = \mathfrak{a}$. This means that we have a mapping

$$\tilde{\sigma} : k[a, \ldots \sigma^d(a)] \mapsto k[a, \ldots, \sigma^{d+1}(a)],$$

such that $\tilde{\sigma}_{|k[a,\ldots,\sigma^{d-1}(a)]} = \sigma$. Then $(\ker(\sigma)) \subseteq \ker(\tilde{\sigma})$, which immediately yields Equation (4) if we take the intersection with $k[a, \ldots, \sigma^{d-1}(a)]$. □

The condition $(\ker(\sigma)) \cap k[a, \ldots, \sigma^{d-1}(a)] = \ker(\sigma)$ thus suffices to find a prime prolongation of a prime kernel. The next example, however, shows that this condition does not suffice to ensure the existence of a realization. This is another aspect which is different from the known case of reflexive prime kernels.

Example 4.17. *Let $\mathbb{Q}$ be a σ-field and consider the difference polynomial ring $\mathbb{Q}\{y_1, y_2\}$. The ideal*

$$\mathfrak{a} = (\sigma^2(y_2) + 1, \sigma^2(y_1)y_2 + \sigma(y_1)y_2 + \sigma^2(y_1) + \sigma(y_1) + y_2) \trianglelefteq \mathbb{Q}\{y_1, y_2\}[2]$$

is a prime kernel, as can be verified by a calculation using [9]. For $\mathfrak{a}$, if we consider the factor ring $\mathbb{Q}\{y\}[2]/\mathfrak{a} =: \mathbb{Q}[a, \sigma(a), \sigma^2(a)]$, the kernel of $\sigma : \mathbb{Q}[a, \sigma(a)] \to \mathbb{Q}[a, \sigma(a), \sigma^2(a)]$ satisfies that

$$(\ker(\sigma)) \cap \mathbb{Q}[a, \sigma(a)] = \ker(\sigma).$$

However, similarly to the case in Example 4.11, any difference ideal of $\mathbb{Q}\{y\}$ containing $\mathfrak{a}$ has to contain 1 and thus be already the whole ring $\mathbb{Q}\{y\}$. The commented code for this example can be found in Appendix A.

We see then, that the condition $(\ker(\sigma)) \cap k[a, \ldots, \sigma^{d-1}(a)] = \ker(\sigma)$, while sufficient for finding a single prime prolongation, is not sufficient for finding a realization; the problem occurs when trying to find a prolongation of the prolongation. This motivates the following conjecture:

Conjecture 4.18. *Let k be a σ-field and $\mathfrak{a} \subseteq k\{y\}[d]$ a prime σ-kernel of length d. Let $a_1 = y_1 + \mathfrak{a}, \ldots, a_n = y_n + \mathfrak{a}$. For $r \geq 1$ consider the mapping*

$$\sigma^r : k[a, \sigma(a), \ldots, \sigma^{d-r}(a)] \to k[a, \ldots, \sigma^d(a)], f \mapsto \sigma^r(f).$$

Then there exists a principal realization of $\mathfrak{a}$, if and only if

$$(\ker(\sigma), \ldots, \ker(\sigma^r)) \cap k[a, \ldots, \sigma^{d-r}(a)] = \ker(\sigma^r).$$

Since in the difference polynomial ring $k\{y\}$, σ is an endomorphism of the ring, the powers of σ are well-defined on all $k\{y\}$ and are difference operators as well. These powers thus remain endomorphisms if we factor out a prime difference ideal $\mathfrak{p}$. For $r \in \mathbb{N}$ it is obvious that $\ker(\sigma^r) \subseteq \ker(\sigma^{r+1})$. This means that in the factor ring $k\{a\}[d] := (k\{y\}/\mathfrak{p})[d]$ we have

$$(\ker(\sigma), \ldots, \ker(\sigma^r)) = \ker(\sigma^r).$$

This means we can show the implication "$\Rightarrow$". The question if the other direction is true remains open.

4.2 A Geometric Application of Difference Kernels

There is an application of difference kernels that is of a geometric nature. We will simply quote a result for the case of reflexive prime kernels here, and do a partial generalization for the case that arises for some non-necessarily-reflexive prime σ-ideals. We obtain the geometrical result stated in the introduction.

Theorem 4.19. *Let k be a σ-field and let $\mathfrak{p} \trianglelefteq_\sigma k\{y\} = k\{y_1, \ldots, y_n\}$ be a prime σ-ideal of $k\{y\}$. For $i \in \mathbb{N}$ set*

$$d_i := \dim(k\{y\}[i]/\mathfrak{p}[i]).$$

Then there exist integers $d, e \in \mathbb{N}$, such that $d_i = d(i+1) + e$ for $i \gg 0$.

Proof. See Theorem 5.1 of [1]. □

Definition 4.20. *Let k be a σ-field and $\mathfrak{p} \trianglelefteq_\sigma k\{y_1, \ldots, y_n\}$ be a prime σ-ideal. Further, let $d, e \in \mathbb{N}$ be as in Theorem 4.19. We call d the* σ-dimension *of $\mathfrak{p}$, or the* σ-dimension *of the irreducible σ-m-variety $X := \mathbb{V}(\mathfrak{p})$ and denote it by $\sigma\text{-dim}(\mathfrak{p})$ and $\sigma\text{-dim}(X)$, respectively. The other quantity, e, we call the* σ-degree *of $\mathfrak{p}$ or X and us the symbol σ-deg for it. Finally, we can combine the information of both in a so-called* dimension polynomial $\omega_\mathfrak{p}(i) := d(i+1)+e$, *which then gives the dimension of $\mathfrak{p}[i]$ for i large enough.*

Recall from the introductory Section, Theorem 1.25:

Theorem 1.25. Let k be a σ-field and $f \in k\{y_1, \ldots, y_n\}$, $f \notin k$ an irreducible σ-polynomial, such that $\text{Eord}(f) = \text{Ord}(f)$. Then the σ-variety $\mathbb{V}(f) \subset \mathbb{A}_k^n$ has an irreducible component X, such that $\sigma\text{-dim}(X) = n - 1$ and $\sigma\text{-deg}(X) = \text{Ord}(f)$.

While this statement is a very interesting result, it falls short quickly, as soon as the difference polynomial f does not satisfy $\text{Eord}(f) = \text{Ord}(f)$. This can be seen already in a very simple example.

Example 4.21. *Consider the σ-polynomial ring $\mathbb{Q}\{y_1\}$. The σ-polynomial $f := \sigma(y_1)-1$ is obviously irreducible. The σ-variety $X := \mathbb{V}(f)$ has only one prime component, namely $[y_1 - 1]$, since $[y_1 - 1] = \{\sigma(y_1 - 1)\}$ is σ-prime. The dimension polynomial of X is $\omega_X(i) = 0$, since $\mathbb{Q}\{y_1\}[i]/([y_1-1][i]) \cong \mathbb{Q}$ for all i. However, the order of f is 1, which means that Theorem 1.25 does not work for f.*

Theorem 4.22. *Let k be a σ-field and $f \in k\{y_1, \ldots, y_n\}$, $f \notin k$ an irreducible σ-polynomial. Then the σ-m-variety $\mathbb{V}(f) \subset \mathbb{A}_k^n$ has an irreducible closed subset X such that $\sigma\text{-dim}(X) = n - 1$ and $\sigma\text{-deg}(X) = \text{Ord}(f)$.*

Proof. Consider the σ-polynomial ring $k\{\sigma^d(y)\} =: k\{z\}$, where d is maximal, such that $f \in k\{\sigma^d(y)\}$ (i.e., $d = \text{Ord}(f) - \text{Eord}(f)$). We let $f' \in k\{z\}$ be the σ-polynomial corresponding to f. Since f is irreducible, f' has to be irreducible as well. Additionally, by definition of d, it has to hold that $\text{Eord}_z(f') = \text{Ord}_z(f')$, where the order is considered with respect to z, as indicated by the subscript.

By Theorem 1.25 we know that the σ-variety $\mathbb{V}(f')$ has an irreducible component $X' = \mathbb{V}(\mathfrak{p})$ of σ-dimension $n - 1$ and σ-degree $\text{Ord}_z(f')$. In other words, there exists a σ-prime difference ideal $\mathfrak{p} \trianglelefteq_\sigma k\{z\}$ minimal over $\{f'\} \trianglelefteq_\sigma k\{z\}$ with $\sigma\text{-dim}(\mathfrak{p}) = n - 1$ and $\sigma\text{-deg}(\mathfrak{p}) = \text{Ord}_z(f')$.

Now, we assert that the ideal $(\mathfrak{p})$ generated by $\mathfrak{p}$ in $k\{y\}$ is a prime difference ideal. To prove this, let $f = \sum_{i=1}^r f_i p_i \in (\mathfrak{p})$, with $p_i \in \mathfrak{p}$; $f_i \in k\{y\}$ for all i. Then, since $\mathfrak{p}$ is a difference ideal, it has to be that $\sigma(p_i) \in \mathfrak{p}$ for

all i. This, in turn, implies that $\sigma(f) = \sum_{i=1}^{r} \sigma(f_i)\sigma(p_i) \in (\mathfrak{p})$. Thus, $(\mathfrak{p})$ is a difference ideal in $k\{y\}$.

Now we can show the primality of $(\mathfrak{p})$. As rings,

$$k\{y\} \cong k[y, \ldots, \sigma^{d-1}(y)] \otimes_k k\{z\}.$$

From Lemma 4.12 it then follows that

$$(k[y, \ldots, \sigma^{d-1}(y)] \otimes_k k\{z\})/(\mathfrak{p}) \cong k\{z\}/\mathfrak{p} \otimes_k k[y, \ldots, \sigma^{d-1}(y)]. \tag{7}$$

Since $\mathfrak{p}$ is prime, $k\{z\}/\mathfrak{p}$ is an integral domain. This implies that $(k\{z\}/\mathfrak{p}) \otimes_k k[y, \ldots, \sigma^{d-1}(y)]$ is an integral domain. Equation (7) then implies that $(\mathfrak{p}) \trianglelefteq_\sigma k\{y\}$ is prime as well.

We only have to compare the dimension polynomials of $\mathfrak{p}$ (over $k\{z\}$) and $(\mathfrak{p})$ over $k\{y\}$. For this, we first consider the isomorphism

$$\begin{aligned} \varphi : k\{y\} &\xrightarrow{\sim} k[y, \ldots, \sigma^{d-1}(y)] \otimes_k k\{z\}, \\ (y, \ldots, \sigma^{d-1}(y)) &\mapsto (y, \ldots, \sigma^{d-1}(y)); \sigma^d(y) \mapsto z. \end{aligned}$$

For any $f \in k\{\sigma^d(y)\}$ we have the property that $\mathrm{Ord}_y(f) = \mathrm{Ord}_z(\varphi(f)) + d$ (where Ord_z is only defined on the subset $\varphi(k\{\sigma^d(y)\}) = k\{z\}$ of the ring $k\{z\} \otimes_k k[y, \ldots, \sigma^{d-1}(y)]$). In particular, this means that φ commutes with the operation of restricting to the i-th power of σ, in the following sense: For a subset $F \subseteq k\{y\}$ and $i > d$ we have

$$\begin{aligned} \varphi(F[i]) &= \varphi(k\{y\}[i] \cap F) = \varphi(k\{y\}[i]) \cap \varphi(F) \\ &= (k[y, \ldots, \sigma^{d-1}(y)] \otimes_k k\{z\}[i-d]) \cap \varphi(F). \end{aligned}$$

If we apply this to $\mathfrak{p}$, we get that for $i \geq 0$, $\varphi((\mathfrak{p})[i+d]) = k[y, \ldots, \sigma^{d-1}(y) \otimes_k \mathfrak{p}[i]$, and thus

$$k\{y\}[i+d]/(\mathfrak{p})[i+d] \cong \underbrace{k[y, \ldots, \sigma^{d-1}(y)]}_{\dim = d \cdot n} \otimes_k k\{z\}[i]/\mathfrak{p}[i].$$

This implies that

$$\dim(k\{y\}[i+d]/(\mathfrak{p})[i+d]) = \dim(k\{z\}[i]/\mathfrak{p}[i]) + nd.$$

By definition of σ-deg and σ-dim, we can conclude that

$$\begin{aligned} (i+d+1)\sigma\text{-}\dim((\mathfrak{p})) &= \omega_{(\mathfrak{p})}(i+d) = \omega_{\mathfrak{p}}(i) + dn \\ &= (i+1)\underbrace{\sigma\text{-}\dim(\mathfrak{p})}_{=n-1} + \underbrace{\sigma\text{-}\deg(\mathfrak{p})}_{\mathrm{Ord}(f')} + dn \end{aligned}$$

It follows that

$$\sigma\text{-}\dim((\mathfrak{p})) = \sigma\text{-}\dim(\mathfrak{p}) = n - 1,$$

as well as

$$\sigma\text{-}\deg((\mathfrak{p})) = \sigma\text{-}\deg(\mathfrak{p}) + d = \mathrm{Ord}(f') + d = \mathrm{Ord}(f).$$

Since $f \in (\mathfrak{p})$ and $(\mathfrak{p})$ is a prime difference ideal, the inclusion $\{f\}_m \subseteq (\mathfrak{p})$ is obvious, which in terms of the σ-m-varieties means that $\mathbb{V}(\mathfrak{p}) \subset \mathbb{V}(f)$.

□

Example 4.23. *We can return to the example of the σ-polynomial $f = \sigma(y_1) - 1$ in the ring $\mathbb{Q}\{y_1\}$. The σ-m-variety $X := \mathbb{V}(f)$ has only one prime component as well, namely $[\sigma(y_1 - 1)]$, since $[\sigma(y_1 - 1)] = \{\sigma(y_1 - 1)\}_m$ is prime. However, the dimension polynomial of X is $\omega_X(i) = 1$, since $\mathbb{Q}\{y_1\}[i]/([\sigma(y_1) - 1][i]) \cong \mathbb{Q}[y_1]$ for all i, in accordance to Theorem 4.22.*

This theorem shows an application of the theory developed for mixed difference ideals, where in this generalization we do not need any restriction on the order of the difference polynomial. It is not a complete generalization however, as it remains unclear if the irreducible closed subset given by the theorem is maximal, in other words, an irreducible component of $\mathbb{V}(f)$.

A Code for the Examples in Macaulay2

In this appendix we give the code used for calculating two examples in the thesis with its corresponding output. We do this with brief commentary in between to make it easier to understand.

A.1 Example 4.11

We consider the difference polynomials

$$f_1 := \sigma(y_2)+1, f_2 := \sigma(y_1)y_2+y_1y_2+\sigma(y_1)+y_1+y_2 \in \mathbb{Q}[y_1, y_2, \sigma(y_1), \sigma(y_2)] =: R.$$

For the calculations we considered the rational numbers $\mathbb{Q}$ as a constant σ-field. We begin by defining the ring R:

```
i1 : R = QQ[s2y_1,s2y_2,sy_1,sy_2,y_1,y_2]

o1 = R

o1 : PolynomialRing
```

The definition is that of a simple polynomial ring, and we just take the names of the variables in a way we can easily interpret them as powers of σ applied to a variable. We add one more power of σ as in the example, so that we can calculate the relation stated later, which includes σ^2. The output, which can be recognized from the lines beginning with an "o", indicates that a polynomial ring has been successfully constructed. We continue and define the ideal.

```
i2 : I = ideal(sy_2+1,sy_1*y_2 + y_1*y_2 + sy_1 + y_1 + y_2)

o2 = ideal (sy   + 1, sy y  + y y  + sy   + y   + y )
             2         1 2    1 2     1     1     2

o2 : Ideal of R
```

Macaulay conveniently has a function to test if the ideal is prime:

```
i3 : isPrime(I)

o3 = true
```

This, however, does not necessarily mean that the ideal is a prime kernel. To see this, we use Gröbner bases.

```
i4 : groebnerBasis(I)
```

```
o4 = | sy_2+1 sy_1y_2+y_1y_2+sy_1+y_1+y_2 |

              1        2
o4 : Matrix R  <-- R

i5 : y_1 < sy_1

o5 = true
```

It tells us that f_1, f_2 is a Gröbner basis of I. The variable ordering is per default graded reverse lexicographical with respect to the input. We tested it here as an example to make sure it was as intended. Using elimination theory (see for example Theorem 2 in Chapter 3 of [11]), we thus see that $(f_1, f_2)[0] = \{0\}$.

Finally, we use Macaulay to test the relation given in the example.

```
i6 : (sy_2+1)*(s2y_1+ sy_1 + 1)- (s2y_1*sy_2 + sy_1*sy_2 + s2y_1
     + sy_1 + sy_2)

o6 = 1

o6 : R
```

A.2 Example 4.17

This second example is a bit more complex, since we have to check the condition that

$$(\ker(\sigma)) \cap \mathbb{Q}[a, \sigma(a)] = \ker(\sigma).$$

We begin again by defining the ring we will work with

```
i1 :  D = QQ[s2y_1 ,s2y_2 ,sy_1 ,sy_2 ,y_1 ,y_2]

o1 = D

o1 : PolynomialRing
```

This time, we want to consider a quotient ring, so we begin by defining the subring $DM1 = \mathbb{Q}[y_1, y_2, \sigma(y_1), \sigma(y_2)]$.

```
i2 :  (DM1, i) = selectVariables(new List from 2..5 ,D)

o2 = (DM1, map(D,DM1,{sy  , sy  , y  , y  }))
                       1    2    1    2
```

```
o2 : Sequence
```

We return to use our original ring and define the ideal we want to factor out.

```
i3 : use D

o3 = D

o3 : PolynomialRing

i4 :  I = ideal(s2y_2+1,s2y_1*y_2 + sy_1*y_2 + s2y_1 + sy_1 +
     y_2)

o4 = ideal (s2y   + 1, s2y y  + sy y  + s2y  + sy  + y )
              2          1 2     1 2      1     1    2

o4 : Ideal of D

i5 :  groebnerBasis I

o5 = | s2y_2+1 s2y_1y_2+sy_1y_2+s2y_1+sy_1+y_2 |

             1        2
o5 : Matrix D  <--- D


i6 : isPrime(I)

o6 = true
```

From the Gröbner basis we again see that I is indeed a prime kernel, since $I[1] = 0$. Now we can define the quotient ring D/I.

```
i7 : F2 = D/I

o7 = F2

o7 : QuotientRing
```

Now we proceed to define the mapping σ. Since $I \cap \mathbb{Q}\{y\}[1] = \{0\}$ we know that $\mathbb{Q}[a, \sigma(a)] \cong \mathbb{Q}[y, \sigma(y)]$ and can use the latter for defining σ. Since $I[1] = 0$, the factor ring $F1 := \mathbb{Q}\{y\}[1]/I[1] \cong \mathbb{Q}\{y\}[1]$, so we can define them to be equal.

```

```

```
i8 : F1 = DM1

o8 = DM1

o8 : PolynomialRing

i9 : use F1

o9 = DM1

o9 : PolynomialRing

i10 :  sigma = map(F2,F1,{y_1 => F2_(symbol sy_1),y_2 => F2_(
    symbol sy_2), sy_1 => F2_(symbol s2y_1), sy_2 => F2_(symbol
    s2y_2)})

o10 = map(F2,DM1,{s2y  , -1, sy  , sy  })
                   1         1     2

o10 : RingMap F2 <-- DM1
```

With this output Macaulay2 tells us that it successfully defined the mapping. We can look at its kernel now.

```
i11 :  groebnerBasis kernel(sigma)

o11 = | sy_2+1 |

                1          1
o11 : Matrix DM1  <-- DM1
```

We see that $\ker(\sigma) = (\sigma(y_2) + 1) \trianglelefteq \mathbb{Q}[y_1, y_2, \sigma(y_1), \sigma(y_2)]$. From this we should be able to already deduce that the condition holds, but we can ask Macaulay to explicitly calculate it too, by going back to the polynomial ring.

```
i12 : use D

o12 = D

o12 : PolynomialRing

i13 : H = ideal(sy_2 + 1, s2y_2 + 1, s2y_1 * y_2 + sy_1*y_2 +
    s2y_1 + sy_1 + y_2)

o13 = ideal (sy  + 1, s2y  + 1, s2y y  + sy y  + s2y  + sy  + y
    )
              2          2          1 2     1 2      1     1    2
```

```
o13 : Ideal of D

i14 : groebnerBasis H

o14 = | sy_2+1 s2y_2+1 s2y_1y_2+sy_1y_2+s2y_1+sy_1+y_2 |

               1         3
```

Which, using elimination theory again, gives the desired result, namely

$$(\ker(\sigma)) \cap \mathbb{Q}[y_1, y_2, \sigma(y_1), \sigma(y_2)] = (\sigma(y_2) + 1) = \ker(\sigma).$$

5 References

[1] Wibmer, Michael *Algebraic Difference Equations (Lecture Notes)*, Available online: `http://www.algebra.rwth-aachen.de/de/Mitarbeiter/Wibmer/Algebraic%20difference%20equations.pdf`

[2] Lang, Serge, *Algebra*, Revised Third Edition, Springer, 2005

[3] Eisenbud, David *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, 1995

[4] Hartshorne, Robin *Algebraic Geometry*, Springer, 1977

[5] Cohn, Richard *Difference Algebra*, Interscience Publishers, 1965

[6] Levin, Alexander *Difference Algebra*, Springer, 2008

[7] Hrushovski, Ehud *The Elementary Theory of the Frobenius Automorphism*, arXiv:math/0406514

[8] Bourbaki, Nicolas *Commutative Algebra*, Hermann, 1972

[9] Grayson, Daniel R. and Stillman, Michael E., Macaulay2, a software system for research in algebraic geometry, Available at http://www.math.uiuc.edu/Macaulay2/

[10] Levin, Alexander, *On the ascending chain condition for mixed difference ideals*, arXiv:1207.4721

[11] Cox, Little and O'Shea, *Ideals, Varieties and Algorithms*, Second Edition, Springer, 1997

Index