Roswitha Rissner, Dipl.-Ing.

Integer-valued polynomials

DISSERTATION

zur Erlangung des akademischen Grades

Doktorin der technischen Wissenschaften

eingereicht an der

Technischen Universität Graz

Betreuerin:
Ao.Univ.-Prof. Mag.rer.nat. Dr.techn. Sophie Frisch

Institut für Analysis und Computational Number Theory (Math A)

Graz, Juni 2015

EIDESSTATTLICHE ERKLÄRUNG

AFFIDAVIT

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Dissertation identisch.

I declare that I have authored this thesis independently, that I have not used other sources and resources than the ones declared, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present doctoral dissertation.

Datum/Date

Unterschrift/Signature

Contents

Acknowledgments

First, I would like to thank my advisor Sophie Frisch for giving me the opportunity to conduct my doctoral studies under her supervision. I also want to express my gratitude to Paul-Jean Cahen for his patience and guidance during our joint work. I am grateful for the opportunity to work with him. Special thanks are also extended to Jean-Luc Chabert and Wolfgang Herfort; their thorough proofreading and helpful suggestions are greatly appreciated. Further, my thanks are extended to my colleagues at Graz University of Technology and at Karl-Franzens University Graz, for many useful discussions and for their support during the course of my studies. Especially, I want to thank Robert Tichy and Hermine Panzenböck for always having an open door for me. Moreover, I would like thank the Austrian Science Fund (FWF) for the financial support.

And finally, I thank my friends and family for their constant support and encouragement. In particular, I would like to thank my parents without whom none of this would have been possible.

Preface

This PhD thesis comprises a collection of publications of the author. After a general introduction to the topic of this thesis, there are two chapters, each reprinting one paper. The first article is submitted while the second is already published. A complete list of publications of the author can be found in the next chapter. This list contains also two articles which are not part of this thesis.

List of publications

[I] P.-J. Cahen and R. Rissner. *Finiteness and Skolem closure of ideals for non-unibranched domains. Communications in Algebra* 43 (2015), pp. 2231–2239. doi: 10.1080/00927872.2013.879159.

[II] R. Rissner. *Null ideal of matrices over residue class rings of principal ideal domains. Submitted* (2015).

[III] R. Rissner and R. E. Burkard. *Bounds on the radius and status of graphs. Networks* 64.2 (2014), pp. 76–83. issn: 0028-3045. doi: 10.1002/net.21558.

[IV] R. E. Burkard and R. Rissner. *Polynomially solvable special cases of the quadratic bottleneck assignment problem. J. Comb. Optim.* 22.4 (2011), pp. 845–856. issn: 1382-6905. doi: 10.1007/s10878-010-9333-7.

1 Introduction

The classical ring of integer-valued polynomials is the ring of polynomials with rational coefficients mapping $\mathbb{Z}$ to $\mathbb{Z}$, that is,

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}.$$

This ring has many interesting properties and has been extensively investigated. It is probably one of the most natural examples of a non-Noetherian domain. It is indeed a two-dimensional Prüfer domain. Further, as a $\mathbb{Z}$-module, it is generated by the so-called binomial polynomials $\binom{X}{n}$ which are $\mathbb{Z}$-linearly independent. While integer-valued polynomials occur much earlier in the literature, it was Skolem who first investigated $\mathrm{Int}(\mathbb{Z})$ as a ring (not only as $\mathbb{Z}$-module), see [24]. He pointed out a property of $\mathrm{Int}(\mathbb{Z})$ which today is referred to as *Skolem property*: If $g_1, \ldots, g_n \in \mathrm{Int}(\mathbb{Z})$ are polynomials such that the values $g_1(z), \ldots, g_n(z)$ are coprime in $\mathbb{Z}$ for all $z \in \mathbb{Z}$, then the polynomials generate the whole ring $\mathrm{Int}(\mathbb{Z})$ (as ideal in $\mathrm{Int}(\mathbb{Z})$). This does not hold for polynomials in $\mathbb{Z}[X]$; the values of the polynomials 2 and $X^2 + X + 1$ are coprime for all integers z, but the ideal of $\mathbb{Z}[X]$ which is generated by 2 and $X^2 + X + 1$ is strictly contained in $\mathbb{Z}[X]$. However, in $\mathrm{Int}(\mathbb{Z})$ an even stronger property holds, the so-called *strong Skolem property.* The finitely generated ideals of $\mathrm{Int}(\mathbb{Z})$ are characterized by their ideals of values, that is, $\mathfrak{A}(m) = \{f(m) \mid f \in \mathfrak{A}\}$ for an ideal $\mathfrak{A}$ of $\mathrm{Int}(\mathbb{Z})$ and an integer $m \in \mathbb{Z}$. To be more specific, let $\mathfrak{A}$ and $\mathfrak{B}$ be two finitely generated ideals of $\mathrm{Int}(\mathbb{Z})$, then $\mathfrak{A} = \mathfrak{B}$ if and only if $\mathfrak{A}(m) = \mathfrak{B}(m)$ for all $m \in \mathbb{Z}$.
Many generalizations of $\mathrm{Int}(\mathbb{Z})$ occur in the literature and are subject of extensive research over the last few decades. This thesis addresses two of them. There is a specific introduction for both of them, in Sections 1.1 and 1.2, where an overview and a summary of the results of this thesis are given.

One way is to extend the definition of $\mathrm{Int}(\mathbb{Z})$ to an arbitrary domain D with quotient field K. Then the ring of integer-valued polynomials is defined as

$$\mathrm{Int}(D) = \{f \in K[X] \mid f(D) \subseteq D\}.$$

This ring has been investigated over the last decades and many of its properties are well-understood. For an extensive treatment see [6]. It is common to assume the domain D to be Noetherian in this context. Then $\mathrm{Int}(D)$ behaves well with respect to localization which often allows to assume that D is local. Further, it turned out that $\mathrm{Int}(D)$ shows its most interesting behavior, if D has Krull dimension one and its residue field is finite. For details on these assumptions, see Section 1.2.
However, even if D is a one-dimensional, Noetherian domain, $\mathrm{Int}(D)$ does not always satisfy the (strong) Skolem property. When investigating Skolem properties of $\mathrm{Int}(D)$, it

is possible to split the ideals of $\mathrm{Int}(D)$ into two categories, the ideals which contain non-zero constants, and those ideals whose intersection with D is equal to $\mathbf{0}$. We concentrate on *almost* (strong) Skolem properties here, that is, if we restrict the investigation of Skolem properties to ideals which contain non-zero constants, the so-called *unitary* ideals. It has been known, for about 30 years, that if the ring on integer-valued polynomials is dense in the ring $\mathcal{C}(\widehat{D}, \widehat{D})$ of $\mathfrak{m}$-adically continuous functions on the $\mathfrak{m}$-adic completion $\widehat{D}$ of D, then $\mathrm{Int}(D)$ satisfies the almost strong Skolem property. If this sufficient condition is satisfied, we say that $\mathrm{Int}(D)$ has the *Stone-Weierstrass property.* However, whether the reverse implication holds is still an open question. In the paper contained in Chapter 3, which is joint work with Paul-Jean Cahen, the authors address this question and determine necessary restrictions on D for $\mathrm{Int}(D)$ to satisfy the almost strong Skolem property. To this end, the authors have a closer look at the ideals

$$\mathfrak{M}_{k,a} = \{f \in \mathrm{Int}(D) \mid f(a) \in \mathfrak{m}^k\}$$

of $\mathrm{Int}(D)$ for $a \in D$. It is shown that these ideals are not finitely generated for all $k \geq 1$. In particular, the maximal ideals of $\mathrm{Int}(D)$ of the form $\mathfrak{M}_a = \{f \in \mathrm{Int}(D) \mid f(a) \in \mathfrak{m}\}$ for $a \in D$ are not finitely generated. In case these ideals are all distinct, this result has been known before. However, we give a proof which holds without this assumption, cf. Chapter 3. A more detailed introduction to this topic can be found in Section 1.2.

For a further generalization, let $\mathrm{M}_n(D)$ be the ring of $n \times n$ square matrices with entries in a domain D with quotient field K. The ring of integer-valued polynomials on $\mathrm{M}_n(D)$ is the set of all polynomials in $K[X]$ which are integer-valued on the D-algebra $\mathrm{M}_n(D)$, that is,

$$\mathrm{Int}(\mathrm{M}_n(D)) = \{f \in K[X] \mid f(\mathrm{M}_n(D)) \subseteq \mathrm{M}_n(D)\}.$$

This generalization of integer-valued polynomials is rather young and can be seen as a special case of integer-valued polynomials on D-algebras. For literature on this topic the reader is referred to [10], [12], [13], [16], [19] and [20].

The work of the author in this context concerns the overring of $\mathrm{Int}(\mathrm{M}_n(D))$ of integer-valued polynomials on a single matrix $A \in \mathrm{M}_n(D)$, that is,

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \{f \in K[X] \mid f(A) \subseteq \mathrm{M}_n(D)\}.$$

Apart from the description of the elements in $\mathrm{Int}(A, \mathrm{M}_n(D))$, the question which matrices in $\mathrm{M}_n(D)$ are images of A under polynomials in $K[X]$ were a strong motivation for the investigation of Chapters 2. There is a natural connection between integer-valued polynomials on a single matrix and the null ideal of a matrix over residue class rings of a given domain which is explained later-on, in Section 1.1.1 of this introduction. The null ideal of a matrix is a well-known notion which has its origins in classical linear algebra. Given a ring R and a square matrix A over R, the null ideal of A is the set of all polynomials $f \in R[X]$ such that $f(A) = 0$. In Chapter 2 which contains the article [22], the author determines a generating set for the null ideal in case $R = {}^{D}\!/_{dD}$ is the residue class ring of a principal ideal domain D modulo $d \in D$. Two applications of this result are discussed. The knowledge of a generating set for the null ideal of a matrix modulo $d \in D$ allows to give an explicit description of $\operatorname{Int}(A, \mathrm{M}_n(D))$. Further, it can be used to compute a decomposition of the ${}^{D}\!/_{dD}$-module ${}^{D}\!/_{dD}[[A]_d]$ into cyclic summands where $[A]_d$ is the image of A under the projection modulo d. A more detailed introduction to null ideals of matrices follows in the next section.

1.1 Null ideal of matrices over commutative rings

Let R be a commutative ring and $A \in \mathrm{M}_n(R)$. The *null ideal of A* is defined as

$$\mathcal{N}_R(A) = \{f \in R[X] \mid f(A) = 0\}.$$

This is a well-known notion in classical linear algebra, that is, if the underlying ring R is a field. In this case $R[X]$ is a principal ideal domain, and therefore $\mathcal{N}_R(A)$ is generated by a single polynomial. In particular, there is a uniquely determined monic polynomial μ_A such that $\mathcal{N}_R(A) = \mu_A R[X]$. This polynomial is called the *minimal polynomial of A*.

However, over general commutative rings, only little is known about the null ideal of a matrix. As the famous Cayley-Hamilton Theorem holds over any commutative ring, the null ideal of A always contains the characteristic polynomial χ_A of A. In particular, it always contains a monic polynomial. It turns out that monic polynomials in $\mathcal{N}_R(A)$ of minimal degree play a special role. We call a monic polynomial $f \in R[X]$ a *minimal polynomial of A over R* if $f \in \mathcal{N}_R(A)$ and $\deg(f) \leq \deg(g)$ for all monic polynomials $g \in \mathcal{N}_R(A)$. (Note that this definition is consistent with the classical definition of minimal polynomials if R is a field.) Unlike their degree, minimal polynomials of matrices over general commutative rings have no uniqueness properties.

It is known that if R is a domain, then the null ideal of every square matrix is a principal ideal if and only if R is integrally closed (see Brown [3], Frisch [11]). Note that for a domain R, $\mathcal{N}_R(A)$ is principal if and only if $\mu_A \in D[X]$ (where μ_A is the minimal polynomial of A over the quotient field of R). In particular, μ_A is a monic divisor of χ_A over the quotient field of R and therefore in $D[X]$, if D is integrally closed, cf. [1, Ch. 5, §1.3, Prop. 11]. For the reverse implication, Frisch constructed a matrix whose minimal polynomial has a coefficient which is equal to a given element of the integral closure of R.

Brown investigated the null ideal of matrices over general commutative rings, see [3] ,[4] and [5]. In the first two papers, he investigated the relationship between the null ideal of a matrix A and the null ideal of a spanning rank partner of A. The *spanning rank* is the smallest number r such that $A = PQ$ is the product of an $(n \times r)$-matrix P and an $(r \times n)$-matrix Q. It is a generalization of the classical rank of a matrix over a field. The $(r \times r)$-matrix QP is called a *spanning rank partner* of A. In the third paper, Brown addressed the question under what conditions the null ideal of a matrix is principal. He gives some sufficient conditions on certain submodules of the null ideal for it to be principal. He also showed that the null ideal of every (2×2)-matrix is principal if and only if the underlying ring is P.P. Further he shows that, if the underlying ring R has only finitely many minimal prime ideals, then the null ideal of every square matrix is principal if and only if R is a finite product of integrally closed domains.

If we consider a matrix over a domain, then there is always the possibility to consider the matrix over the quotient field, which allows to use the tools of classical linear algebra. However, if the underlying ring R is not a domain this is no longer possible.

In Chapter 2, we assume $R = {}^{D}\!/_{dD}$ to be the residue class ring of a principal ideal domain D modulo $d \in D$. It suffices to consider prime powers of D, that is, $d = p^\ell$ for $p \in D$ a prime element and $\ell \in \mathbb{N}$. Theorem 2.3.15 describes a generating set of the null ideal of A modulo p^ℓ with at most ℓ elements. This generating set has various interesting properties. In particular, it is connected to the ${}^{D}\!/_{p^\ell D}$-module decomposition of ${}^{D}\!/_{p^\ell D}[[A]_{p^\ell}]$ (where $[A]_{p^\ell} \in \mathrm{M}_n({}^{D}\!/_{p^\ell D})$ is the image of A under projection modulo p^ℓ). Although it remains an open question whether the determined generating set is minimal, its relationship to the invariant factors of ${}^{D}\!/_{p^\ell D}[[A]_{p^\ell}]$ emphasizes its usefulness, see Theorem 2.4.5.

1.1.1 Integer-valued polynomials on a single matrix

As mentioned above, there is a natural connection between integer-valued polynomials and null ideals. Let D be a domain with quotient field K and $A \in \mathrm{M}_n(D)$. If $f \in K[X]$, then there exists $g \in D[X]$ and $d \in D$ such that $f = \frac{g}{d}$. Therefore $f \in \mathrm{Int}(A, \mathrm{M}_n(D))$ is equivalent to $g(A) \in d\,\mathrm{M}_n(D)$ which, in turn, is equivalent to $g(A) \equiv 0 \mod d$. If $[\,.\,]_d$ denotes the residue class modulo d, then for all $g \in D[X]$ and $d \in D \setminus \{0\}$

$$\frac{g}{d} \in \mathrm{Int}(A, \mathrm{M}_n(D)) \quad \Longleftrightarrow \quad [g]_d \in \mathcal{N}_{D/dD}([A]_d)$$

The author shows in Chapter 2, that there exists a finite set $\mathcal{P}_A$ of prime elements of D and natural numbers m_p such that

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \mu_A K[X] + D[X] + \sum_{p \in \mathcal{P}_A} \frac{1}{p^{m_p}} \mathsf{N}_{p^{m_p}}(A)$$

where $\mathsf{N}_d(A)$ denotes $\{f \in D[X] \mid [f]_d \in \mathcal{N}_{D/dD}([A]_d)\}$ for $d \in D$, and $\mu_A \in D[X]$ is the minimal polynomial of A over K.

1.2 The ring $\mathrm{Int}(D)$

Let D be a domain with quotient field K and $D \neq K$. The ring of integer-valued polynomials on D is defined as

$$\mathrm{Int}(D) = \{f \in K[X] \mid f(D) \subseteq D\} \tag{1.2.1}$$

In general, $D[X] \subseteq \mathrm{Int}(D) \subsetneq K[X]$ holds. Without question, we want to avoid the case $\mathrm{Int}(D) = D[X]$ when investigating the ring of integer-valued polynomials on D. Although the polynomial ring over D in one variable has nice and interesting properties, its investigation can be done without any relation to integer-valued polynomials. We say $\operatorname{Int}(D)$ is trivial if $\operatorname{Int}(D) = D[X]$.

A useful observation is the following. Let $f \in \operatorname{Int}(D)$ be a polynomial of degree n and $a_0, a_1, \dots, a_n \in D$ be pairwise distinct elements. Then the coefficients $f_i \in K$ of $f = \sum_{i=0}^{n} f_i X^i$ are a solution to the following system of linear equations:

$$A\mathbf{x} = \begin{pmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^n \\ 1 & a_1 & a_1^2 & \cdots & a_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^n \end{pmatrix} \mathbf{x} = \begin{pmatrix} f(a_0) \\ f(a_1) \\ \vdots \\ f(a_n) \end{pmatrix} \in D^n$$

Note that $A \in \mathrm{M}_{n+1}(D)$, and so is its adjugate matrix $A^{\#}$ and therefore

$$\det(A)\mathbf{x} = A^{\#}A\mathbf{x} = A^{\#} \begin{pmatrix} f(a_0) \\ f(a_1) \\ \vdots \\ f(a_n) \end{pmatrix} \in D^n$$

Note that A is a Vandermonde matrix, hence $d = \det(A) = \prod_{i<j}(a_i - a_j) \in D$. Since the coefficients f_i of f are a solution to the system, it follows in particular, that $df_i \in D$ and therefore $df \in D[X]$.

However, if $\mathfrak{p}$ is a prime ideal with infinite residue class ring $D/\mathfrak{p}$, then we can choose $a_0, a_1, \dots, a_n \in D$ to be pairwise not congruent modulo $\mathfrak{p}$. Hence $d = \prod_{i<j}(a_i - a_j) \notin \mathfrak{p}$ and therefore $f_i \in D_{\mathfrak{p}}$. In particular, if $D/\mathfrak{p}$ is infinite, then

$$\operatorname{Int}(D) \subseteq D_{\mathfrak{p}}[X] \tag{1.2.2}$$

holds, cf. [6, Corollary I.3.7].

It is common to assume that D is a Noetherian domain. Then $\operatorname{Int}(D)$ behaves well with respect to localization. To be more specific, if S is a multiplicative subset of D, then

$$S^{-1}\operatorname{Int}(D) = \operatorname{Int}(S^{-1}D)$$

To understand this equality, we first show $f(S^{-1}D) \subseteq S^{-1}D$ for $f \in \operatorname{Int}(D)$. This is done by induction on the degree of f. It is clear for constant polynomials in $\operatorname{Int}(D)$. Hence let $f \in \operatorname{Int}(D)$ be a polynomial of degree n, and assume that the assertion holds for all polynomials in $\operatorname{Int}(D)$ of degree less than n. For $s \in S$, we set $g(X) = s^n f(X) - f(sX)$. Then $g \in \operatorname{Int}(D)$ of degree less than n and therefore $g(S^{-1}D) \subseteq S^{-1}D$. Then $s^n f(\frac{a}{s}) = g(\frac{a}{s}) + f(a) \in S^{-1}D$ for $a \in D$. Therefore $S^{-1}\operatorname{Int}(D) \subseteq \operatorname{Int}(S^{-1}D)$ holds (even in the non-Noetherian case). For the reverse inclusion, let $f \in \operatorname{Int}(S^{-1}D)$. If D is Noetherian, then the D-module generated by the coefficients of f is a Noetherian module. Since ${}_D\langle f(D)\rangle$ is a D-submodule of this module, it is finitely generated. However,

$f(D) \subseteq S^{-1}D$, and thus there exists $s \in S$ such that $sf(D) \in D$, cf. [6, Theorem I.2.3]. Hence $sf \in \operatorname{Int}(D)$. In particular, for any prime ideal $\mathfrak{p}$ of D

$$\operatorname{Int}(D)_{\mathfrak{p}} = \operatorname{Int}(D_{\mathfrak{p}})$$

holds. Therefore it is often convenient to assume D to be local with maximal ideal $\mathfrak{m}$. Further we ask $D/\mathfrak{m}$ to be finite, since otherwise $\operatorname{Int}(D) = D[X]$, see Equation (1.2.2). In addition, it is common to assume that D has Krull dimension one, when investigating $\operatorname{Int}(D)$. Otherwise $D[X] \subseteq \operatorname{Int}(D) \subseteq D'[X]$ where D' is the integral closure of D. This is in some sense less interesting, for example if D is integrally closed, then $\operatorname{Int}(D)$ is trivial.
Assume for a moment that the Krull dimension of D is higher than one, then, so is the Krull dimension of D'. In general, $\operatorname{Int}(D)$ is not contained in $\operatorname{Int}(D')$ but they are both subrings of $\operatorname{Int}(D, D') = \{f \in K[X] \mid f(D) \subseteq D'\}$. If, however, the Krull dimension of D' is higher than one, then we can show that

$$D'[X] = \operatorname{Int}(D') = \operatorname{Int}(D, D')$$

and therefore

$$D[X] \subseteq \operatorname{Int}(D) \subseteq \operatorname{Int}(D, D') = D'[X].$$

To understand these equations, observe that the integral closure D' of D is always a Krull domain according to the Mori-Nagata Theorem (cf. [21]). In particular, this implies that D' is the intersection of the localizations $D'_{\mathfrak{P}}$ of D' at all prime ideals $\mathfrak{P}$ of D' of height one. Further, for every prime ideal $\mathfrak{P}$ of D' of height one, the ideal $\mathfrak{p} = \mathfrak{P} \cap D$ is a prime ideal of D of height one. And since D is local with maximal ideal $\mathfrak{m}$, it follows that $\mathfrak{p} \neq \mathfrak{m}$. In particular, $D/\mathfrak{p}$ is infinite. Let $f \in \operatorname{Int}(D, D')$ with $\deg(f) = n$, then there exist $a_0, \ldots, a_n \in D$ such that a_i and a_j are not congruent modulo $\mathfrak{p} = \mathfrak{P} \cap D$ for $i \neq j$. Therefore, we can use the "Vandermonde" argumentation from the beginning of this section, to conclude that $f \in D'_{\mathfrak{P}}[X]$ and hence

$$D'[X] \subseteq \operatorname{Int}(D') \subseteq \operatorname{Int}(D, D') \subseteq \bigcap_{\mathfrak{P} \in \mathcal{P}} D'_{\mathfrak{P}}[X] = D'[X]$$

We say D is polynomially dense in D' if $\operatorname{Int}(D, D') = \operatorname{Int}(D')$, cf. [6, Corollary IV.4.10].

1.2.1 Characterization of Noetherian, one-dimensional, local domains

Convention 1.2.1. For the reasons explained in the previous subsection, we assume that D is a Noetherian, one-dimensional, local domain with maximal ideal $\mathfrak{m}$ and finite residue field $D/\mathfrak{m}$.

Let D' be the integral closure of D. Then D' is Noetherian and has Krull dimension one according to the Krull-Akizuki Theorem, cf. [17, Theorem 11.7]. Further, every maximal ideal of D' is a minimal prime overideal of $\mathfrak{m}D'$ and therefore there are only finitely many of them. Hence D' is a semilocal Dedekind domain. In the context of integer-valued polynomials it is worth mentioning, that if $D/\mathfrak{m}$ is finite, then the residue class fields of D' are finite as well, which follows from the Krull-Akizuki Theorem.

Definition 1.2.2. We say D is *unibranched* if D' is local.

Let $\widehat{D}$ denote the $\mathfrak{m}$-adic completion of D. It is well-known that $\widehat{D}$ may not be a domain. In particular, if D is non-unibranched, then it is possible to construct non-zero zero-divisors in $\widehat{D}$ explicitly. Hence if $\widehat{D}$ is a domain, then D is necessarily unibranched. However, the reverse implication does not hold in general, cf. Theorem 1.2.4.

Definition 1.2.3. We say D is *analytically unramified* if the $\mathfrak{m}$-adic completion $\widehat{D}$ is reduced. We say D is *analytically irreducible*, if $\widehat{D}$ is a domain.

Note that if D' is local, then it is a discrete valuation domain (with maximal ideal $\mathfrak{m}'$). Further, observe that the completion of a discrete valuation domain (w.r.t. to its maximal ideal) is again a discrete valuation domain, hence discrete valuation domains are analytically irreducible.

Analytically irreducible domains play a special role in the context of integer-valued polynomials. This is due to the fact that integer-valued polynomials on D are continuous functions in the $\mathfrak{a}$-adic topology where $\mathfrak{a}$ is an ideal of D. Therefore, $\mathrm{Int}(D)$ is contained in the ring $\mathcal{C}(\widehat{D}, \widehat{D})$ of continuous functions on $\widehat{D}$ ($\mathfrak{a} = \mathfrak{m}$). This leads to the question whether $\mathrm{Int}(D)$ satisfies the analogue of the Stone-Weierstrass Theorem. We say $\mathrm{Int}(D)$ has the *Stone-Weierstrass property* if $\mathrm{Int}(D)$ is dense in $\mathcal{C}(\widehat{D}, \widehat{D})$ with respect to the uniform convergence topology. It turns out (see [6, Theorem III.5.3]) that $\mathrm{Int}(D)$ has the Stone-Weierstrass property if and only if D is analytically irreducible. This has some interesting implication in the context of Skolem properties which is explained in Section 1.2.3.

The following theorem is a characterization of analytically irreducible domains, cf. [6, Proposition III.5.2], [18, (43.20)] and [18, (32.2)].

Theorem 1.2.4. *Let D be a Noetherian, one-dimensional, local domain. Then the following assertions are equivalent:*

(a) D is analytically irreducible.

(b) D is analytically unramified and unibranched.

(c) D is unibranched and the integral closure D' of D is finitely generated as D-module.

(d) D is unibranched and, if $\mathfrak{m}'$ denotes the maximal ideal of D', then the $\mathfrak{m}'$-adic topology of D' induces the $\mathfrak{m}$-adic topology on D.

Assume D' to be local with maximal ideal $\mathfrak{m}'$, and let $\widehat{D'}$ be the $\mathfrak{m}'$-adic completion of D'. Further, let $\overline{D}$ be the topological closure of D in $\widehat{D'}$. The ring $\overline{D}$ is the completion of D with respect to the subspace topology on D which is induced by the $\mathfrak{m}'$-adic topology on D'. Figure 1.1 below demonstrates the relationship between D, D' and the completions with respect to the different topologies. We can assume $D \subseteq \widehat{D}$ and $D' \subseteq \widehat{D'}$ since the corresponding topologies are Hausdorff. Then $D \subseteq \widehat{D'}$ and therefore $D \subseteq \overline{D} \subseteq \widehat{D'}$ holds. Hence the lines in Figure 1.1 represent inclusions. However, the dotted arrow is a ring homomorphism φ from $\widehat{D}$ to $\overline{D}$ which deserves some additional explanation.

Observe, that the inclusion $D \hookrightarrow \overline{D}$ is a uniformly continuous homomorphism (where D is equipped with the $\mathfrak{m}$-adic topology). Hence, by the universal property of $\widehat{D}$, this inclusion induces a uniquely determined continuous extension $\varphi : \widehat{D} \to \overline{D}$. To be more specific, recall that the $\mathfrak{m}$-adic completion of D is isomorphic (as topological ring) to the projective limit $\varprojlim D/\mathfrak{m}^n$ of the system $(D/\mathfrak{m}^n)_{n\in\mathbb{N}}$ together with the natural projections. Analogously, the completion $\overline{D}$ of D with respect to the $\mathfrak{m}'$-adic subspace topology is isomorphic to the projective limit $\varprojlim D/(\mathfrak{m}'^n \cap D)$. The family of the natural homomorphisms $\varphi_n : D/\mathfrak{m}^n \to D/(\mathfrak{m}'^n \cap D)$ for $n \in \mathbb{N}$ is a homomorphism of projective systems, that is, the diagram

$$\begin{tikzcd}
D/\mathfrak{m}^n \arrow[r, "\varphi_n"] \arrow[d] & D/(\mathfrak{m}'^n \cap D) \arrow[d] \\
D/\mathfrak{m}^{n-1} \arrow[r, "\varphi_{n-1}"] & D/(\mathfrak{m}'^{n-1} \cap D)
\end{tikzcd}$$

commutes for all $n \in \mathbb{N}$. Therefore $(\varphi_n)_{n\in\mathbb{N}}$ induces a uniformly continuous ring homomorphism $\varphi : \widehat{D} \to \overline{D}$. According to Theorem 1.2.4, D is analytically irreducible if and only if φ is an isomorphism ($\widehat{D} \simeq \overline{D}$).

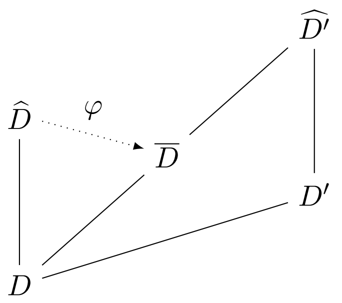

Figure 1.1: $\mathfrak{m}$-adic and $\mathfrak{m}'$-adic completions of D and D' in case D is unibranched

As stated below, if D is analytically irreducible, then $\mathrm{Int}(D)$ satisfies the almost strong Skolem property. Chapter 3 of this thesis presents necessary conditions for $\mathrm{Int}(D)$ to satisfy the almost strong Skolem property. It turns out, that the almost strong Skolem property of $\mathrm{Int}(D)$ implies that D is unibranched, see Theorem 3.4.3.

1.2.2 The spectrum of $\mathrm{Int}(D)$

Recall that $\mathrm{Int}(D)$ behaves well w.r.t. localization (at least if D is Noetherian), that is, $\mathrm{Int}(D)_\mathfrak{p} = \mathrm{Int}(D_\mathfrak{p})$. Hence, the prime ideals of $\mathrm{Int}(D)$ lying over (0) can be easily described since they correspond to the prime ideals of $\mathrm{Int}(D)_{(0)} = \mathrm{Int}(K) = K[X]$. Therefore, the non-zero prime ideals lying over (0) are in one-to-one correspondence to the monic, irreducible polynomials of $K[X]$. They are all of the form

$$\mathfrak{P}_q = qK[X] \cap \mathrm{Int}(D)$$

for irreducible, monic polynomials $q \in K[X]$, cf. [6, Corollary V.1.2]. Further, since we assume D to be Noetherian, one-dimensional and local, the prime spectrum of D contains only (0) and $\mathfrak{m}$. It remains to describe the prime ideals of $\mathrm{Int}(D)$ which lie above $\mathfrak{m}$. As integer-valued polynomials are $\mathfrak{m}$-adically continuous, we can consider them as continuous functions on the $\mathfrak{m}$-adic completion $\widehat{D}$ of D. For $\alpha \in \widehat{D}$, the set

$$\mathfrak{M}_\alpha = \{f \in \mathrm{Int}(D) \mid f(\alpha) \in \widehat{\mathfrak{m}}\}$$

is an ideal of $\mathrm{Int}(D)$. It is maximal, since it is the kernel of the ring epimorphism

$$\begin{aligned} \varphi_\alpha : \mathrm{Int}(D) &\longrightarrow \widehat{D}/\widehat{\mathfrak{m}} \\ f &\longmapsto f(\alpha) + \widehat{m} \end{aligned}$$

and $\widehat{D}/\widehat{\mathfrak{m}} \simeq D/\mathfrak{m}$ is a field. In fact, all prime ideals of $\mathrm{Int}(D)$ lying over $\mathfrak{m}$ are of this form (and are thus maximal), see [6, Proposition V.2.2]. If D is analytically irreducible, then the maximal ideals of $\mathrm{Int}(D)$ of the form $\mathfrak{M}_\alpha$ for $\alpha \in \widehat{D}$ are all distinct, that is, $\mathfrak{M}_\alpha \neq \mathfrak{M}_\beta$ for $\alpha \neq \beta$. This is due to the Stone-Weierstrass property: If D is analytically irreducible, then $\mathrm{Int}(D)$ is dense in the ring $\mathcal{C}(\widehat{D}, \widehat{D})$ of continuous functions on $\widehat{D}$ w.r.t. the uniform convergence topology. Therefore, for $\alpha \neq \beta$, there exists an integer-valued polynomial $f \in \mathrm{Int}(D)$ such that $f(\alpha) \in \widehat{\mathfrak{m}}$ and $f(\beta) \notin \widehat{\mathfrak{m}}$. In particular, this implies $\mathfrak{M}_\alpha \neq \mathfrak{M}_\beta$.
However, if D is unibranched, but not analytically irreducible, then the ideals of the form $\mathfrak{M}_\alpha$ for $\alpha \in \widehat{D}$ are not necessarily distinct. In this case, it is possible to exploit the fact that the integral closure D' of D is a discrete valuation domain (since it is local) and therefore analytically irreducible. Let $\mathfrak{m}'$ be the maximal ideal of D'. If $\overline{D}$ is the topological closure of D in the $\mathfrak{m}'$-adic completion $\widehat{D'}$ of D', then the prime ideals of $\mathrm{Int}(D)$ lying over $\mathfrak{m}$ correspond to the elements of $\overline{D}$. As the polynomials in $\mathrm{Int}(D)$ are $\mathfrak{m}'$-adically continuous, it is possible to write all the prime ideals of $\mathrm{Int}(D)$ above $\mathfrak{m}$ as

$$\mathfrak{M}_\alpha = \{f \in \mathrm{Int}(D) \mid f(\alpha) \in \widehat{\mathfrak{m}'}\}$$

for $\alpha \in \overline{D}$, cf. [6, Theorem V.3.1]. Note that, in case that D is analytically irreducible, we have $\widehat{D} \simeq \overline{D}$, by Theorem 1.2.4 of the previous section.
And finally, if D is not unibranched, then there are only finitely many prime ideals of $\mathrm{Int}(D)$ lying over $\mathfrak{m}$. In fact, there exists a non-zero ideal $\mathfrak{q}$, the so-called *equalizing ideal*, such that $\mathfrak{M}_a = \mathfrak{M}_b$ if and only if $a \equiv b \mod \mathfrak{q}$. Since D is one-dimensional, Noetherian and local, there exists a power $\mathfrak{m}^k$ of $\mathfrak{m}$ which is contained in $\mathfrak{q}$. Due to this and the finiteness of $D/\mathfrak{m}$ (see Convention 1.2.1), the residue class ring $D/\mathfrak{q}$ is finite, cf. [6, Proposition V.3.10].
Regarding the non-finiteness of the ideals $\mathfrak{M}_a$ with $a \in D$, observe the following: If D is unibranched, then the ideals of the form $\mathfrak{M}_a$ are distinct for distinct $a \in D$. Assume $\mathfrak{M}_a = (f_1, \ldots, f_r)$ to be finitely generated. Then, since the polynomials f_i are $\mathfrak{m}$-adically continuous, $f_i(a) \in \mathfrak{m}$ implies that there exists a neighborhood U of a such that $f_i(b) \in \mathfrak{m}$ for all $1 \leq i \leq r$ and all $b \in U$. However, this implies that $\mathfrak{M}_a \subseteq \mathfrak{M}_b$, and hence $\mathfrak{M}_a = \mathfrak{M}_b$ for all $b \in U$ which is impossible.
In paper [8], reprinted in Chapter 3, the authors show, that the ideals of the form $\mathfrak{M}_a$ for $a \in D$ are not finitely generated, even in the non-unibranched case. For this purpose,

a generalized notion of the equalizing ideal is studied. Further, this allows to prove that there always exists a power $\mathfrak{m}^k$ such that the ideals of the form $\mathfrak{M}_{k,a} = \{f \in \operatorname{Int}(D) \mid f(a) \in \mathfrak{m}^k\}$ are distinct. Then, it is possible to show (with the same arguments as above), that these ideals are not finitely generated which then allows to deduce the maximal ideals $\mathfrak{M}_a$ are not finitely generated, cf. Theorem 3.4.2.

1.2.3 Skolem properties

As mentioned at the beginning of this introduction, the finitely generated ideals of $\operatorname{Int}(\mathbb{Z})$ can be characterized by their ideals of values. Skolem pointed out the following property of $\operatorname{Int}(\mathbb{Z})$, which today is referred to as *Skolem property*: let $f_1, \dots, f_n \in \operatorname{Int}(\mathbb{Z})$ be integer-valued polynomials on $\mathbb{Z}$. If for every integer $z \in \mathbb{Z}$, the ideal of $\mathbb{Z}$ generated by the values $f_1(z), \dots, f_n(z)$ is equal to $\mathbb{Z}$, then $f_1, \dots, f_n$ already generate $\operatorname{Int}(\mathbb{Z})$. To be accurate, Skolem proved this statement more generally for integer-valued polynomials in finitely many variables. In his proof, he constructs integer-valued polynomials $h_1, \dots, h_n$, such that $\sum_{i=1}^{n} h_i f_i = 1$. However, in $\operatorname{Int}(\mathbb{Z})$ an even stronger property holds: let $f_1, \dots, f_n, g_1, \dots, g_m \in \operatorname{Int}(\mathbb{Z})$ be integer-valued polynomials on $\mathbb{Z}$. If for every integer $z \in \mathbb{Z}$, the ideal of $\mathbb{Z}$ generated by the values $f_1(z), \dots, f_n(z)$ is equal to the ideal generated by $g_1(z), \dots, g_m(z)$, then the ideal $(f_1, \dots, f_n)$ of $\operatorname{Int}(\mathbb{Z})$ is equal to $(g_1, \dots, g_m)$. This is usually referred to as the *strong Skolem property.* Note that the polynomial ring $\mathbb{Z}[X]$ satisfies neither of these properties.

The motivation for investigating Skolem properties is the question to what extend (finitely generated) ideals can be characterized by their ideals of values. To be more specific, let $\mathfrak{A}$ be an ideal of $\operatorname{Int}(D)$. Then the *ideal of values of* $\mathfrak{A}$ *at* $a \in D$ is the ideal

$$\mathfrak{A}(a) = \{f(a) \mid f \in \mathfrak{A}\}$$

of D. Further the *Skolem closure of* $\mathfrak{A}$ is defined as

$$\mathfrak{A}^\star = \{f \in \operatorname{Int}(D) \mid \forall a \in D : f(a) \in \mathfrak{A}(a)\}$$

We say that $\mathfrak{A}$ is *Skolem closed* if $\mathfrak{A} = \mathfrak{A}^\star$.

For the investigation of Skolem properties, one can consider two types of ideals of $\operatorname{Int}(D)$ separately, which are those that contain non-zero constants (the *unitary* ideals), and those whose intersection with D is equal to $\mathbf{0}$, see [6, Chapter VII.2].

Definition 1.2.5. 1. We say that $\operatorname{Int}(D)$ has the *(almost) Skolem property*, if for each finitely generated (unitary) ideal $\mathfrak{A}$ of $\operatorname{Int}(D)$, $\mathfrak{A}^\star = \operatorname{Int}(D)$ implies $\mathfrak{A} = \operatorname{Int}(D)$.

2. We say that $\operatorname{Int}(D)$ satisfies the *(almost) strong Skolem property*, if each finitely generated (unitary) ideal $\mathfrak{A}$ of $\operatorname{Int}(D)$ is Skolem closed.

Alternatively, one refers to D as an ((almost) strong) Skolem ring, if $\operatorname{Int}(D)$ has the respective Skolem property.

It is worth mentioning here that the Skolem property does not localize. If D is a local domain, and $t \in \mathfrak{m}$ is a non-zero non-unit of D, we set $\mathfrak{A} = (1 + tX)$. Then for all $a \in D$, the equality $\mathfrak{A}(a) = D$ holds, but $\mathfrak{A} \neq \operatorname{Int}(D)$. (The same argument actually shows that all domains with non-zero Jacobson radical are not Skolem.) However, observe that the ideal $\mathfrak{A}$ is not unitary. The Skolem properties of non-unitary ideals are connected to d-rings. A ring is called d-ring, if each integer-valued rational function on D is actually an (integer-valued) polynomial. It has been shown, that D is a (strong) Skolem ring if and only if D is an almost (strong) Skolem d-ring, see [6, Proposition VII.2.14].

The paper reprinted in Chapter 3, deals apart from its results on the non-finiteness of some maximal ideals of Int(D) with almost strong Skolem properties. While the tool of localization is not applicable for (strong) Skolem properties, it is useful when investigating almost (strong) Skolem properties.

It has been known since the 1980s, that if D is, in addition to the usual assumptions, analytically irreducible (and therefore Int(D) has the Stone-Weierstrass property), then Int(D) has the almost strong Skolem property [6, Theorem VII.3.9]. However, it is unknown if the reverse implication is also true. In Chapter 3, the authors prove, that almost strong Skolem rings are necessarily unibranched, that is, the integral closure D' of D is local (and hence a discrete valuation domain).

2 Null ideal of matrices over residue class rings of principal ideal domains

This chapter contains the article [22] with the title *Null ideal of matrices over residue class rings of principal ideal domains*. The article is submitted.

2.1 Abstract

Given a square matrix A with entries in a commutative ring S, the ideal of $S[X]$ consisting of polynomials f with $f(A) = 0$ is called the null ideal of A. Very little is known about null ideals of matrices over general commutative rings. We compute a generating set of the null ideal of a matrix in case $S = {}^{D}\!/_{dD}$ is the residue class ring of a principal ideal domain D modulo $d \in D$. We discuss two applications. At first, we compute a decomposition of the S-module $S[A]$ into cyclic S-modules and explain the strong relationship between this decomposition and the determined generating set of the null ideal of A. And finally, we give a rather explicit description of the ring $\mathrm{Int}(A, \mathrm{M}_n(D))$ of all integer-valued polynomials on A.

Keywords. null ideal, matrix, minimal polynomial, integer-valued polynomials

2.2 Introduction

Matrices with entries in commutative rings arise in numerous contexts, both in pure and applied mathematics. However, many of the well-known results of classical linear algebra do not hold in this general setting. This is the case even if the underlying ring is a domain (but not a field). For a general introduction to matrix theory over commutative rings we refer to the textbook of Brown [2].

The purpose of this paper is to provide a better understanding of the null ideal of square matrices over residue class rings of principal ideal domains. The *null ideal* $\mathcal{N}_S(A)$ of a square matrix A over a commutative ring S is the set of all polynomials which annihilate A, that is,

$$\mathcal{N}_S(A) = \{f \in S[X] \mid f(A) = 0\}.$$

In case S is a field, it is well-known that the null ideal of A is generated by a uniquely determined monic polynomial, the so-called *minimal polynomial* μ_A of A. Further it is known that if S is a domain, then the null ideal of every square matrix is principal (generated by μ_A) if and only if S is integrally closed, (Brown [3], Frisch [11]). However, little is known about the null ideal of a matrix with entries in a commutative ring. The well-known Cayley-Hamilton Theorem states that every square matrix over a commutative ring satisfies its own characteristic equation (cf. [15, Theorem XIV.3.1]). Therefore there always exists a monic polynomial in $S[X]$ of minimal degree which annihilates the matrix.

Definition 2.2.1. Let $A \in \mathrm{M}_n(S)$ be a square matrix over a commutative ring S. If $f \in S[X]$ is a monic polynomial with $f(A) = 0$ and there exists no monic polynomial in $S[X]$ of smaller degree with this property, then we call f a *minimal polynomial* of A over S.

Note that, in case S is a field, the definition above is consistent with the classical definition of the (uniquely determined) minimal polynomial of a square matrix. However in general, if S is not a field, a minimal polynomial of a matrix over S is not uniquely determined, but its degree is. It is known that if S is a domain, then the null ideal of A is principal if and only if A has a uniquely determined minimal polynomial over S, which is in turn equivalent to the (uniquely determined) minimal polynomial μ_A of A over the quotient field of S being in $S[X]$.

Brown discusses conditions for the null ideal to be principal over a general commutative ring R (with identity). In [5], he gives sufficient conditions on certain $R[X]$-submodules of the null ideal for the null ideal to be principal. In addition, he shows that the null ideal of every (2×2)-matrix over R is principal if and only if R is a P.P. ring. Further he proves, if R contains only finitely many minimal prime ideals, then this is in turn equivalent to R being a finite direct product of domains. He also proves that (if R contains only finitely many minimal primes), then the null ideal of every square matrix is principal if and only if R is a finite product of integrally closed domains. There is also earlier work of Brown investigating the relationship of the null ideal $\mathcal{N}(A)$ of a matrix A and the null ideal $\mathcal{N}(B)$ of a *spanning rank partner* B of A over a commutative ring, see [3], [4]. The *spanning rank* is a generalization of the classical rank of a matrix over a field. It is the smallest integer r, such that $A = PQ$ is the product of an $(n\times r)$-matrix P and an $(r\times n)$-matrix Q. The matrix $B = QP$ is called a spanning rank partner of A. Brown shows, for example, that if the underlying ring is a domain, then either $\mathcal{N}(A) = \mathcal{N}(B)$, $\mathcal{N}(A) = X\mathcal{N}(B)$ or $X\mathcal{N}(A) = \mathcal{N}(B)$ (where X is the indeterminate of the polynomial ring).

A better understanding of the null ideal of matrices over residue class rings of domains has applications in the theory of integer-valued polynomials on matrix rings. Let D be a domain with quotient field K, and let $A \in \mathrm{M}_n(D)$. For a polynomial $f \in K[X]$, the image $f(A)$ of A under f is a matrix with entries in K. There are two immediate questions in this context: The action of which polynomials is integer-valued on A, that is, for which $f \in K[X]$ does $f(A) \in \mathrm{M}_n(D)$ hold? And what are the images of A under these polynomials? We set

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \{f \in K[X] \mid f(A) \in \mathrm{M}_n(D)\}$$

the ring of integer-valued polynomials on A, and we denote by

$$\mathrm{Int}(A, \mathrm{M}_n(D))(A) = \{f(A) \mid f \in \mathrm{Int}(A, \mathrm{M}_n(D))\}$$

the ring of images of A under integer-valued polynomials of A. $\mathrm{Int}(A, \mathrm{M}_n(D))$ is an overring of the ring of integer-valued polynomials on the D-algebra $\mathrm{M}_n(D)$, that is,

$$\mathrm{Int}(\mathrm{M}_n(D)) = \{f \in K[X] \mid f(\mathrm{M}_n(D)) \subseteq \mathrm{M}_n(D)\}$$

The ring $\mathrm{Int}(\mathrm{M}_n(D))$ and other generalizations of integer-valued polynomial rings are subject of recent research, see [10], [12], [13], [16], [19] and [20].
For the ring of integer-valued polynomials on a single matrix A, the following inclusion holds

$$\mu_A K[X] + D[X] \subseteq \mathrm{Int}(A, \mathrm{M}_n(D))$$

There are both, instances in which equality holds, and instances in which the inclusion is strict. If equality holds, it is readily seen that $\mathrm{Int}(A, \mathrm{M}_n(D))(A) = D[A]$, that is, all images of A under integer-valued polynomials on A can be written as $g(A)$ with $g \in D[X]$. As far as the images of A are concerned, the integer-valued polynomials in $K[X] \setminus D[X]$ do not contribute anything new in this case. In fact, the reverse implication holds too. Let $f \in \mathrm{Int}(A, \mathrm{M}_n(D))$ and assume that there exists a polynomial $g \in D[X]$ such that $f(A) = g(A)$. Then $f - g$ is an element of the null ideal of A over K, and therefore $f - g = \mu_A h$ for some $h \in K[X]$. In particular, this implies that $f \in \mu_A K[X] + D[X]$. We conclude the following observation.

Observation.

$$\mu_A K[X] + D[X] = \mathrm{Int}(A, \mathrm{M}_n(D)) \quad \Longleftrightarrow \quad \mathrm{Int}(A, \mathrm{M}_n(D))(A) = D[A]$$

Let $f = g\mu_A + h \in \mu_A K[X] + D[X]$ with $g \in K[X]$ and $h \in D[X]$. If $\mu_A \in D[X]$, then we can assume $\deg(h) < \deg(\mu_A)$. Hence, if $f \notin D[X]$, then $f \neq h$ and $g \neq 0$ which implies $\deg(f) \geq \deg(\mu_A)$.
However, in general, $\deg(\mu_A)$ is not a lower bound for the degree of polynomials in $\mathrm{Int}(A, \mathrm{M}_n(D)) \setminus D[X]$. Let $f \in K[X]$, then there exist $g \in D[X]$ and $d \in D$ such that $f = \frac{g}{d}$. Then the following holds:

$$\forall\, d \in D \setminus \{0\} \;\; \forall\, g \in D[X] \; : \left(\frac{g}{d} \in \mathrm{Int}(A, \mathrm{M}_n(D)) \iff g(A) \equiv 0 \mod d\,\mathrm{M}_n(D) \right)$$

which is the case if and only if the residue class of g is in the null ideal of A over the residue class ring ${}^{D}\!/\!{}_{dD}$.
In this paper, we investigate the null ideal of square matrices over the residue class ring ${}^{D}\!/\!{}_{dD}$ of a principal ideal domain D modulo $d \in D$. In Section 2.3 we determine a set of generators of the null ideal of a matrix with entries ${}^{D}\!/\!{}_{dD}$. It turns out that it suffices to consider the special case when $d = p^\ell$ is a prime power ($\ell \in \mathbb{N}$ and $p \in D$ a prime element). The main result of this section is Theorem 2.3.15 which gives an explicit set of generators of the null ideal of a matrix over ${}^{D}\!/\!{}_{p^\ell D}$.
Further we present two applications of the results of Section 2.3. In Section 2.4 we analyze the ${}^{D}\!/\!{}_{p^\ell D}$-module structure of ${}^{D}\!/\!{}_{p^\ell D}[A]$ for $A \in \mathrm{M}_n({}^{D}\!/\!{}_{p^\ell D})$. As a finitely generated module over a principal ideal ring, ${}^{D}\!/\!{}_{p^\ell D}[A]$ decomposes into a direct sum of

cyclic submodules with uniquely determined invariant factors, according to [2, Theorem 15.33]. We compute this decomposition explicitly and find a strong relationship to the generating set of $\mathcal{N}_{D/p^\ell D}(A)$ from Section 2.3.
In the last section we apply the knowledge about the null ideal gained in Section 2.3 to integer-valued polynomials. We give an explicit description of the ring $\mathrm{Int}(A, \mathrm{M}_n(D))$ using ${}^{D}\!/_{p^\ell D}$-minimal polynomials for finitely many prime powers p^ℓ.

2.3 Generators of the null ideal

Throughout this section let D be a principal ideal domain and let $\mathbb{P}$ denote a complete set of representatives of associate classes of prime elements of D. By $\mathsf{lc}(g)$ we denote the leading coefficient of a polynomial $g \in D[X]$. However, we introduce the following notions in a more general setting.
Let S be a commutative ring, I an ideal of S and $A \in \mathrm{M}_n(S)$. Further, we identify the isomorphic rings $\mathrm{M}_n({}^{S}\!/_{I}) = {}^{\mathrm{M}_n(S)}\!/_{I\,\mathrm{M}_n(S)}$ and ${}^{S}\!/_{I}[X] = {}^{S[X]}\!/_{IS[X]}$ and write $[\,.\,]_I$ to denote residue classes modulo I. If $I = (d)$ is a principal domain, then we often write $[\,.\,]_d$ instead of $[\,.\,]_{(d)}$. We set

$$\mathsf{N}_I(A) = \{f \in S[X] \mid f(A) \in I\,\mathrm{M}_n(S)\}$$

Then $\mathcal{N}_{S/I}([A]_I)$ is the image of $\mathsf{N}_I(A)$ under the projection modulo I, that is,

$$\mathcal{N}_{S/I}([A]_I) = \{[f]_I \in {}^{S}\!/_{I}[X] \mid f \in \mathsf{N}_I(A)\}$$

In order to determine the ideal $\mathsf{N}_I(A)$, we introduce a more general notion of a minimal polynomial of A:

Definition 2.3.1. Let S be a commutative ring, I an ideal of S and A a square matrix over S. We say f is an I-minimal polynomial of A (over S), if f is a monic polynomial in $\mathsf{N}_I(A)$ and $\deg(f) \leq \deg(g)$ for all monic polynomials $g \in \mathsf{N}_I(A)$.

Remark 2.3.2. The (0)-minimal polynomials of a matrix A are exactly the minimal polynomials of A over S, cf. Definition 2.2.1. Further, note that the constant polynomial 1 is the uniquely determined S-minimal polynomial of every square matrix A over S ($I = (1) = S$).

Remark 2.3.3. Whether a monic polynomial $f \in S[X]$ is an I-minimal polynomial of A depends only on the residue class of A modulo I. If $I \neq S$ is a proper ideal, then a monic polynomial $f \in S[X]$ is an I-minimal polynomial if and only if its residue class $[f]_I \in {}^{S}\!/_{I}[X]$ is a (0)-minimal polynomial of $[A]_I$ over ${}^{S}\!/_{I}$. (In case $I = S$, one would have to think about the meaning of “monic” polynomial over the null ring to state a similar result. As we do not want to consider the zero polynomial to be monic, we exclude this case.)
Further, let J be an ideal of S such that $J \subseteq I$. Then ${}^{S}\!/_{I} \simeq {}^{(S/J)}\!/_{(I/J)}$. Therefore, f is an I-minimal polynomial of A over S if and only if $[f]_J \in {}^{S}\!/_{J}[X]$ is an ${}^{I}\!/_{J}$-minimal polynomial of $[A]_J$ over ${}^{\mathrm{S}}\!/_{\mathrm{J}}$.

The goal of this section is to compute a generating set for the ideal $\mathsf{N}_I(A)$ of a matrix $A \in \mathrm{M}_n(D)$ over a principal ideal domain D and an ideal I of D. Note that $I = (d)$ for some $d \in D$. We write $\mathsf{N}_d(A)$ instead of $\mathsf{N}_{(d)}(A)$. Moreover, observe that if the leading coefficient of a polynomial $g \in D[X]$ is coprime to d, then it is a unit modulo d. Hence, there exists an element $c \in D$ such that $[cg]_d$ is a monic polynomial in ${}^{D}\!/_{dD}[X]$. In particular, this implies the following lemma.

Lemma 2.3.4. *Let D be a principal ideal domain and $d \notin \{0,1\}$. If $f \in D[X]$ is a (d)-minimal polynomial, then all polynomials $g \in \mathsf{N}_d(A)$ with $\deg(g) < \deg(f)$ have a leading coefficient which is not invertible modulo d, that is, $\gcd(\mathsf{lc}(g), d) \neq 1$.*

Note that $\mathsf{N}_0(A) = \mathcal{N}_D(A)$ is the null ideal of A over D. Further, D is integrally closed, since it is a principal ideal domain. As mentioned in the introduction, this implies that the minimal polynomial of every square matrix in $\mathrm{M}_n(D)$ is in $D[X]$ and generates its null ideal. In particular,

$$\mathsf{N}_0(A) = \mathcal{N}_D(A) = \mu_A D[X]$$

holds, where $\mu_A \in D[X]$ is the minimal polynomial of A over K. This completes the case $d = 0$. For $d \neq 0$, we first observe, that it suffices to compute $\mathsf{N}_d(A)$ for $d = p^\ell$ with $p \in D$ a prime element.

Lemma 2.3.5. *Let D be a principal ideal domain, $A \in \mathrm{M}_n(D)$ and $a, b \in D$ be coprime elements. Then*

$$\mathsf{N}_{ab}(A) = a\,\mathsf{N}_b(A) + b\,\mathsf{N}_a(A)$$

Proof. The inclusion "$\supseteq$" is trivial. For "$\subseteq$", let $g \in \mathsf{N}_{ab}(A)$. Since a and b are coprime, there exist $h_1, h_2 \in D[X]$ such that

$$g = ah_1 + bh_2$$

Then

$$\begin{aligned} a\,h_1(A) &= g(A) - bh_2(A) \in b\,\mathrm{M}_n(D) \text{ and} \\ b\,h_2(A) &= g(A) - ah_1(A) \in a\,\mathrm{M}_n(D) \end{aligned}$$

It follows that $h_1 \in \mathsf{N}_b(A)$ and $h_2 \in \mathsf{N}_a(A)$, which completes the proof. □

Notation and Conventions 2.3.6. For the rest of this section we fix the prime element $p \in D$. If $A \in \mathrm{M}_n(D)$ is fixed, we often write N_{p^ℓ} instead of $\mathsf{N}_{p^\ell}(A)$.

Our goal is to determine polynomials $f_0, \dots, f_m \in D[X]$ such that

$$\mathsf{N}_{p^\ell}(A) = \{f \in D[X] \mid f(A) \equiv 0 \mod (p^\ell)\} = \sum_{i=0}^{m} f_i D[X]$$

for $A \in \mathrm{M}_n(D)$. Since ${}^{D}\!/\!{}_{pD}$ is a field, the null ideal of A modulo p is a principal ideal. Hence

$$\mathsf{N}_p(A) = \nu_1 D[X] + pD[X]$$

where ν_1 is a (p)-minimal polynomial of A. The degree of ν_1 is, by definition, independent of the choice of a (p)-minimal polynomial.

Definition 2.3.7. Let $\nu_1 \in D[X]$ be a (p)-minimal polynomial A. We call $\mathsf{d}_p(A) = \deg(\nu_1)$ *the p-degree of* A and write d_p if the matrix is clear from the context.

Note again, that this definition depends only on the residue class of A modulo p. Observe that the following inclusions hold

$$\mu_A D[X] = \mathcal{N}_D(A) = \mathsf{N}_0 \subseteq \cdots \subseteq \mathsf{N}_{p^\ell} \subseteq \mathsf{N}_{p^{\ell-1}} \subseteq \cdots \subseteq \mathsf{N}_p = \nu_1 D[X] + pD[X] \subseteq D[X] = \mathsf{N}_1$$

where ν_1 is a (p)-minimal polynomial of A. The p-degree of A is a lower bound for the degree of all polynomials in $\mathsf{N}_{p^\ell} \setminus p^\ell D[X]$, as the following lemma states.

Lemma 2.3.8. *Let D be a principal ideal domain, $\ell \geq 1$ and $A \in \mathrm{M}_n(D)$. If $f \in \mathsf{N}_{p^\ell}(A) \setminus p^\ell D[X]$, then* $\deg(f) \geq \mathsf{d}_p(A)$.

Proof. We prove by contradiction. Let $\ell \geq 1$ be minimal such that there exists a polynomial $f \in \mathsf{N}_{p^\ell} \setminus p^\ell D[X]$ with $\deg(f) < \mathsf{d}_p$. Without restriction, we choose f to be a polynomial of minimal degree with this property, that is, if $g \in \mathsf{N}_{p^\ell}$ with $\deg(g) < \deg(f)$, then $g \in p^\ell D[X]$.
If $\ell = 1$, then p divides $\mathsf{lc}(f)$ according to Lemma 2.3.4. Hence $f' = \mathsf{lc}(f) X^{\deg(f)} \in pD[X] \subseteq \mathsf{N}_p$, and therefore $f - f' \in \mathsf{N}_p$ is a polynomial with degree strictly smaller than $\deg(f)$. Therefore $f - f' \in pD[X]$ which implies $f \in pD[X]$, a contradiction.
Hence $\ell > 1$, and since $f \in \mathsf{N}_{p^\ell}$ it follows that $f \in \mathsf{N}_{p^{\ell-1}}$. Then, due to the minimality of ℓ, it follows that $f \in p^{\ell-1} D[X]$. Let $h \in D[X]$ such that $f = p^{\ell-1} h$. Then $\deg(h) = \deg(f) < \mathsf{d}_p$ and

$$f(A) = p^{\ell-1} h(A) \equiv 0 \mod p^\ell$$

which is equivalent to $h \in \mathsf{N}_p$. Then again, by minimality of $\ell > 1$, it follows that $h \in pD[X]$ and therefore $f \in p^\ell D[X]$, contrary to our assumption.

□

The next proposition provides one of the main tools in this section. It states a simple but important result, which allows us to deduce various properties of the generators of N_{p^ℓ}.

Proposition 2.3.9. *Let D be a principal ideal domain, $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$ be a square matrix over D, and ν_ℓ be a (p^ℓ)-minimal polynomial of A (for $\ell \geq 1$). If $f \in \mathsf{N}_{p^\ell}(A)$, then there exist uniquely determined polynomials $q, g \in D[X]$ such that* $\deg(g) < \deg(\nu_\ell)$ *and*

$$f = q\nu_\ell + pg.$$

In particular,

$$\mathsf{N}_{p^\ell}(A) = \nu_\ell D[X] + p\,\mathsf{N}_{p^{\ell-1}}(A).$$

Proof. Let $f \in \mathsf{N}_{p^\ell}$. Since ν_ℓ is monic for every $\ell \geq 1$, we can use polynomial division: there exist uniquely determined $q, r \in D[X]$ with $\deg(r) < \deg(\nu_\ell)$ such that

$$f = q\nu_\ell + r \tag{2.3.1}$$

It is easily seen that $r \in \mathsf{N}_{p^\ell}$, hence it suffices to prove the following claim.

Claim. Let $r \in \mathsf{N}_{p^\ell}$ with $\deg(r) < \deg(\nu_\ell)$. Then $r \in pD[X]$.

If $\ell = 1$, then the assertion follows from Lemma 2.3.8. Let $\ell > 1$ be minimal such that the claim is false. Further, choose $r \in \mathsf{N}_{p^\ell}$ with $\deg(r) < \deg(\nu_\ell)$ of minimal degree such that $r \notin pD[X]$. Since $r \in \mathsf{N}_{p^\ell}$ it is in $\mathsf{N}_{p^{\ell-1}}$ too. By minimality of ℓ, there exist $q', g' \in D[X]$ such that

$$r = q'\nu_{\ell-1} + pg'$$

with $\deg(g') < \deg(\nu_{\ell-1})$. Since $r \notin pD[X]$, it follows that $q' \notin pD[X]$. Therefore, there exists $q_1, q_2 \in D[X]$ with $q_2 \neq 0$ and no non-zero coefficient of q_2 is divisible by p such that

$$q' = pq_1 + q_2$$

Hence r can be written in the following form

$$r = q_1 \underbrace{p\nu_{\ell-1}}_{\in \mathsf{N}_{p^\ell}} + q_2\nu_{\ell-1} + pg' \in \mathsf{N}_{p^\ell}$$

This, however, implies that $f' = q_2\nu_{\ell-1} + pg' \in \mathsf{N}_{p^\ell}$. Observe, that $\deg(g') < \deg(\nu_{\ell-1})$ which implies that $\mathsf{lc}(f') = \mathsf{lc}(q_2)\,\mathsf{lc}(\nu_{\ell-1}) = \mathsf{lc}(q_2)$ is not divisible by p. On the other hand,

$$\deg(f') = \deg(q_2) + \deg(\nu_{\ell-1}) \leq \deg(r) < \deg(\nu_\ell)$$

which implies, by Lemma 2.3.4, that p divides $\mathsf{lc}(f')$, a contradiction. □

We state a corollary of Proposition 2.3.9, which is particularly useful: the smaller the degree of a polynomial in N_{p^ℓ}, the higher the power of p that divides it.

Corollary 2.3.10. *Let D be a principal ideal domain and $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$, $\ell \geq 1$, and ν_j be (p^j)-minimal polynomials of A for $1 \leq j \leq \ell$. If $f \in \mathsf{N}_{p^\ell}(A)$, then*

$$\deg(f) < \deg(\nu_j) \quad \Longrightarrow \quad f \in p^{\ell-(j-1)}D[X]$$

In particular, if $\deg(\nu_\ell) = \deg(\nu_j)$*, then*

$$\mathsf{N}_{p^\ell}(A) = \nu_\ell D[X] + p^{\ell-(j-1)}\mathsf{N}_{p^{j-1}}(A)$$

Proof. We use induction on $\ell \geq 1$. Let $f \in \mathsf{N}_{p^\ell}$ with $\deg(f) < \deg(\nu_j) \leq \deg(\nu_\ell)$. Observe, that $f = pg$ for some $g \in \mathsf{N}_{p^{\ell-1}}$, according to Proposition 2.3.9. Hence if $\ell = j \geq 1$, then the assertion follows. In particular, if $\ell = 1$, then $j = 1$ which proves the basis.
Hence assume $\ell > j > 1$. Then $j \leq \ell - 1$ and we can apply the induction hypothesis to $g \in \mathsf{N}_{p^{\ell-1}}$ and conclude that $g \in p^{\ell-1-(j-1)}D[X]$ which completes the proof. □

At this point, we have enough tools to prove that the polynomials $p^{\ell-i}\nu_i$ generate N_{p^ℓ}. Recall that $\mathsf{N}_1(A) = D[X]$ is generated by the constant polynomial 1, see Remark 2.3.2. Therefore the constant polynomial $\nu_0 = 1$ is the (uniquely determined) (p^0)-minimal polynomial of A for all prime elements p.
We again use induction on ℓ and $\mathsf{N}_1(A) = \mathsf{N}_{p^0}(A) = D[X] = p^0\nu_0 D[X]$ serves as induction basis. The induction step is an application of Proposition 2.3.9.

Theorem 2.3.11. *Let D be a principal ideal domain and $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$ be a square matrix over D, $\ell \geq 0$, and $\nu_j \in D[X]$ be (p^j)-minimal polynomials of A for $0 \leq j \leq \ell$. Then*

$$\mathsf{N}_{p^\ell}(A) = \sum_{j=0}^{\ell} p^{\ell-j}\nu_j D[X]$$

□

Theorem 2.3.11 states that the null ideal N_{p^ℓ} of A is generated by the $\ell+1$ polynomials $p^{\ell-i}\nu_i$ for $0 \leq i \leq \ell$. However, in general this is not a minimal generating set. While we are not able to decide which subsets are minimal generating sets, we can still identify some redundant polynomials in $\{p^{\ell-i}\nu_i \mid 0 \leq i \leq \ell\}$. Note that $\deg(\nu_{i+1}) \geq \deg(\nu_i)$ holds for all $i \geq 0$. It turns out that it suffices to keep one polynomial of each degree in $\{\deg(\nu_i) \mid 0 \leq i \leq \ell\}$ to generate N_{p^ℓ}. Theorem 2.3.15 states explicitly, which subsets of $\{p^{\ell-i}\nu_i \mid 0 \leq i \leq \ell\}$ we might choose. Although the resulting generating set might still not be minimal, it is strongly connected to a certain decomposition of ${}^{D}\!/_{p^\ell D}[[A]_d]$ into cyclic ${}^{D}\!/_{p^\ell D}$-submodules which is the topic of Section 2.4.
Theorem 2.3.11 and Corollary 2.3.10 imply that, if $\deg(\nu_{j+1}) = \deg(\nu_j)$ for some $0 \leq j < \ell$, then N_{p^ℓ} is generated by $\{p^{\ell-i}\nu_i \mid 0 \leq i \leq \ell\} \setminus \{p^{\ell-j}\nu_j\}$, cf. Theorem 2.3.15 below. For each $d \in \{\deg(\nu_i) \mid 0 \leq i \leq \ell\}$ we want to keep only the largest j such that $\deg(\nu_j) = d$. This motivates the following definition.

Definition 2.3.12. Let $A \in \mathrm{M}_n(D)$ be a square matrix with (p^i)-minimal polynomials for $1 \leq i \leq \ell$. Then we call

$$\mathcal{I}_\ell = \{\ell\} \cup \{i \mid 0 \leq i < \ell, \deg(\nu_i) < \deg(\nu_{i+1})\}$$

the *ℓ-th index set of A (w.r.t. the prime element p).*

Remark 2.3.13. The (uniquely determined) degree of a (p^j)-minimal polynomial of A depends only on the residue class of A modulo p^ℓ, not on the choice of a representative.

Remark 2.3.14. The indices 0 and ℓ are always contained in $\mathcal{I}_\ell$. Further, the ℓ-th index set $\mathcal{I}_\ell$ of A satisfies the following:

1. If $\deg \nu_\ell \neq \deg \nu_{\ell-1}$, then $\mathcal{I}_\ell = \{\ell\} \cup \mathcal{I}_{\ell-1}$.
2. If $\deg \nu_\ell = \deg \nu_{\ell-1}$, then $\mathcal{I}_\ell = \{\ell\} \cup (\mathcal{I}_{\ell-1} \setminus \{\ell - 1\})$.

The ℓ-th index set of A contains the information which (p^j)-minimal polynomials we need to generate N_{p^ℓ} as stated by the next theorem.

Theorem 2.3.15. *Let D be a principal ideal domain, $p \in D$ a prime element and $\ell \geq 0$. Further, let $A \in \mathrm{M}_n(D)$ be a square matrix over D with ℓ-th index set $\mathcal{I}_\ell$ and $\nu_i \in D[X]$ be (p^i)-minimal polynomials for $0 \leq i \leq \ell$. Then*

$$\mathsf{N}_{p^\ell}(A) = \sum_{i \in \mathcal{I}_\ell} p^{\ell - i} \nu_i D[X]$$

Proof. We prove this by induction on ℓ. If $\ell = 0$, then $\mathcal{I}_0 = \{0\}$ and the assertion follows from Theorem 2.3.11. Let $\ell \geq 1$. Then $\mathcal{I}_\ell \setminus \{\ell\} \neq \emptyset$; let $k \leq \ell - 1$ be the largest index in $\mathcal{I}_\ell \setminus \{\ell\}$. Then $\deg(\nu_\ell) > \deg(\nu_k)$ and $\deg(\nu_\ell) = \deg(\nu_{k+1})$. Corollary 2.3.10 implies

$$\mathsf{N}_{p^\ell} = \nu_\ell D[X] + p^{\ell - k} \mathsf{N}_{p^k}$$

However, according to the induction hypothesis,

$$\mathsf{N}_{p^k} = \sum_{i \in \mathcal{I}_k} p^{k-i} \nu_i D[X]$$

holds. In addition, it follows from Remark 2.3.14 that $\mathcal{I}_\ell = \mathcal{I}_k \cup \{\ell\}$ which completes the proof. □

Remark 2.3.16. For the general case, let $d = \prod_{i=1}^m p_i^{\ell_i}$ be the prime factorization of an element $d \in D$ and $c_i = \prod_{j \neq i} p_j^{\ell_j}$. Let $\nu_{(p,\ell)}$ denote a (p^ℓ)-minimal polynomial and $\mathcal{I}_{(p,\ell)}$ the ℓ-th index set of A w.r.t. the prime element p. According to Theorem 2.3.15 and Lemma 2.3.5, the following holds:

$$\begin{aligned}\mathsf{N}_d(A) &= \sum_{i=1}^m \left(\sum_{j \in \mathcal{I}_{(p_i,\ell_i)}} c_i \, (p_i^{\ell_i - j} \nu_{(p_i,j)}) D[X] \right) \\ &= \sum_{i=1}^m \left(\sum_{j \in \mathcal{I}_{(p_i,\ell_i)}} \left(\frac{d}{p_i^j} \nu_{(p_i,j)} \right) D[X] \right)\end{aligned}$$

The following assertions are technical observations which are useful later-on.

Corollary 2.3.17. *Let D be a principal ideal domain and $p \in D$ a prime. Further, let $A \in \mathrm{M}_n(D)$ be a square matrix over D with ℓ-th index set $\mathcal{I}_\ell$ (for $\ell \geq 0$) and $\nu_i \in D[X]$ be (p^i)-minimal polynomials of A. If $f \in \mathsf{N}_{p^\ell}(A)$, then*

$$f \in \sum_{i \in \mathcal{I}_\ell^{[f]}} p^{\ell-i} \nu_i \, D[X]$$

where $\mathcal{I}_\ell^{[f]} = \{i \in \mathcal{I}_\ell \mid \deg(\nu_i) \leq \deg(f)\}$.

Proof. We prove this by induction on ℓ. Observe that, if $\deg(f) \geq \deg(\nu_\ell)$, then $\mathcal{I}_\ell^{[f]} = \mathcal{I}_\ell$. In this case the assertion holds, according to Theorem 2.3.15. In particular, this is the case if $\ell = 0$ (which is the induction basis), since $\deg(f) \geq 0 = \deg(\nu_0)$.
Hence assume $\ell \geq 1$ and $\deg(f) < \deg(\nu_\ell)$. Then $\ell \notin \mathcal{I}_\ell^{[f]}$, and according to Corollary 2.3.10, $f = ph$ with $h \in \mathsf{N}_{p^{\ell-1}}$. According to the induction hypothesis, it follows that

$$h \in \sum_{i \in \mathcal{I}_{\ell-1}^{[h]}} p^{\ell-1-i} \nu_i \, D[X]$$

Note that $\deg(f) = \deg(h)$ and therefore $\mathcal{I}_{\ell-1}^{[h]} = \mathcal{I}_{\ell-1}^{[f]}$. We split into two cases, $\deg(\nu_\ell) > \deg(\nu_{\ell-1})$ and $\deg(\nu_\ell) = \deg(\nu_{\ell-1})$. According to Remark 2.3.14, if $\deg(\nu_\ell) > \deg(\nu_{\ell-1})$, then $\mathcal{I}_{\ell-1} \cup \{\ell\} = \mathcal{I}_\ell$. Since $\ell \notin \mathcal{I}_\ell^{[f]}$ it follows that $\mathcal{I}_{\ell-1}^{[f]} = \mathcal{I}_\ell^{[f]}$.
If $\deg(\nu_\ell) = \deg(\nu_{\ell-1})$, then $\mathcal{I}_\ell = \{\ell\} \cup (\mathcal{I}_{\ell-1} \backslash \{\ell-1\})$, by Remark 2.3.14 again. However, $\ell \notin \mathcal{I}_\ell^{[f]}$ and $\ell - 1 \notin \mathcal{I}_{\ell-1}^{[f]}$ since $\deg(f) < \deg(\nu_\ell) = \deg(\nu_{\ell-1})$. Therefore $\mathcal{I}_{\ell-1}^{[f]} = \mathcal{I}_\ell^{[f]}$ in this case too. Hence, in both cases, the following holds

$$f = ph \in \sum_{i \in \mathcal{I}_\ell^{[f]}} p^{\ell-i} \nu_i \, D[X]$$

□

For $i \geq 1$, let $\nu_i \in D[X]$ be (p^i)-minimal polynomials and $\mu_A \in D[X]$ the minimal polynomial of A. Then, by definition,

$$\mathsf{d}_p = \deg(\nu_1) \leq \cdots \leq \deg(\nu_{\ell-1}) \leq \deg(\nu_\ell) \leq \cdots \leq \deg(\mu_A) = \mathsf{d}_A$$

In particular, this sequence of degrees stabilizes. The following proposition states that there always exists an m such that every (p^m)-minimal polynomial has degree d_A, that is, the sequence stabilizes always at the value d_A.

Proposition 2.3.18. *Let D be a principal ideal domain and $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$ with minimal polynomial $\mu_A \in D[X]$ and $\mathsf{d}_A = \deg(\mu_A)$. If ν_i are (p^i)-minimal polynomials of A for $i \geq 0$, then there exists $m \in \mathbb{N}$ such that $\mathsf{d}_A = \deg(\nu_\ell)$ for all $\ell \geq m$.*

Proof. Since $\deg(\nu_i) \leq \deg(\mu_A)$ and $(\deg(\nu_i))_{i \geq 1}$ is a non-decreasing sequence in $\mathbb{N}$, there exists $m \in \mathbb{N}$ such that $\deg(\nu_m) = \deg(\nu_{m+k})$ for all $k \geq 0$. We set $d = \deg(\nu_m)$ and show $d = \mathsf{d}_A$. Note that $d \leq \mathsf{d}_A$, and therefore it suffices to show $d \geq \mathsf{d}_A$.

Since $\nu_{m+k+1} - \nu_{m+k} \in \mathsf{N}_{p^{m+k}}$ is a polynomial with degree less than $\deg(\nu_m)$, it follows from Corollary 2.3.10 that

$$\nu_{m+k+1} - \nu_{m+k} \in p^{k+1}D[X]$$

For $0 \leq i \leq d$, let $a_i^{(k)}$ be the coefficient of X^i of the polynomial ν_{m+k}. Then $(a_i^{(k)})_{k\geq 0}$ are p-adic Cauchy sequences in D. Therefore $\nu = \lim_{k\to\infty} \nu_{m+k}$ is a polynomial over the p-adic completion $\widehat{D}$ of D with coefficients $a_i = \lim_{k\to\infty} a_i^{(k)}$ and $d = \deg(\nu)$. Since, ν_{m+k} is a monic polynomial for all k, it follows that ν is a monic polynomial too.
Further $\nu(A) = 0$, and hence $\nu \in \mathcal{N}_{\widehat{D}}(A)$. Now, let $\widehat{K}$ be the quotient field of $\widehat{D}$. Then $\widehat{K}$ is a field extension of K. Since the minimal polynomial is invariant under field extensions, it follows that $\mathcal{N}_{\widehat{K}}(A) = \mu_A\widehat{K}[X]$. However, $\widehat{D}$ is integrally closed in $\widehat{K}$, and therefore $\mathcal{N}_{\widehat{D}}(A) = \mu_A\widehat{D}[X]$. Therefore $\mu_A \,|\, \nu$ which implies in particular that $\mathsf{d}_A \leq \deg(\nu) = d$. □

We can conclude, that it suffices to determine a finite number of (p^i)-minimal polynomials in order to describe the ideals $\mathsf{N}_{p^\ell}(A)$ for all $\ell \geq 0$.

Corollary 2.3.19. *Let D be a principal ideal domain and $p \in D$ a prime element. Further, let $A \in \mathrm{M}_n(D)$ with (p^i)-minimal polynomials ν_i for $i \geq 0$. Then there exists $m \in \mathbb{N}$ such that for all $k \geq 0$ the following holds:*

$$\mathsf{N}_{p^{m+k}}(A) = \mu_A D[X] + p^k \mathsf{N}_{p^m}(A)$$

Proof. Proposition 2.3.18 implies that there exists an $m \in \mathbb{N}$ such that $\deg(\mu_A) = \deg(\nu_{m+1})$. Then, μ_A is a (p^{m+k+1})-minimal polynomial for all $k \geq 0$ and the assertion follows from Corollary 2.3.10 (with $j = m+1$). □

We conclude this section with an example of a 3×3 matrix over $\mathbb{Z}$. Although we know that (p^ℓ)-minimal polynomials exist, it is not clear how to determine them algorithmically. However, we can compute them for small instances of matrices over $\mathbb{Z}$.

Example 2.3.20. Let $A \in \mathrm{M}_3(\mathbb{Z})$ be defined as follows:

$$A = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 16 & 0 \\ 0 & 0 & 32 \end{pmatrix}$$

Then A has three, pairwise different eigenvalues over $\mathbb{Q}$ and hence

$$\mu_A = (X-4)(X-16)(X-32)$$

is the minimal polynomial of A over $\mathbb{Q}$. Since $\mu_A \in \mathbb{Z}[X]$, it is the (in this case uniquely determined) minimal polynomial (or (0)-minimal polynomial) of A over $\mathbb{Z}$.
Let $p \in \mathbb{Z}$ be a prime element. Recall that we denote the residue classes modulo a prime element p by $[\,.\,]_p$. It is easily seen, that $[A]_p$ has three different eigenvalues in $\mathbb{Z}/p\mathbb{Z}$ for

all prime elements in $\mathbb{Z}$ except for the primes 2, 3 and 7. Therefore, for $p \in \mathbb{P} \setminus \{2,3,7\}$, the polynomial

$$\mu_{[A]_p} = (X - [4]_p)(X - [16]_p)(X - [32]_p) \in {}^{\mathbb{Z}}\!/\!_{p\mathbb{Z}}[X]$$

is the minimal polynomial of $[A]_p$ over ${}^{\mathbb{Z}}\!/\!_{p\mathbb{Z}}$ which implies $\mathsf{d}_p(A) = \deg(\mu_A)$ for all $p \in \mathbb{P} \setminus \{2,3,7\}$. Let $f \in D[X]$ be a (p^ℓ)-minimal polynomial for $\ell \geq 1$, then the inequalities $\mathsf{d}_p(A) \leq \deg(f) \leq \deg(\mu_A)$ hold, cf. Lemma 2.3.8. Therefore μ_A is a (p^ℓ)-minimal polynomial of A and $\{0,\ell\}$ the ℓ-th index set of A w.r.t. the prime p for all prime elements $p \neq 2,3,7$ and all $\ell \geq 1$. Hence, according to Theorem 2.3.15,

$$\forall p \in \mathbb{P} \setminus \{2,3,7\}\ \forall \ell \geq 1: \ \ \mathsf{N}_{p^\ell}(A) = \mu_A\mathbb{Z}[X] + p^\ell\mathbb{Z}[X]$$

The cases $p = 3$ and $p = 7$ are very similar. Therefore, we only handle $p = 3$. The matrix $[A]_3$ has two different eigenvalues in ${}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}}$. Hence

$$\mu_{[A]_3} = (X - [1]_3)(X - [2]_3)$$

is the minimal polynomial of $[A]_3$. One can check (e.g. with a brute force method), that there is no monic polynomial f of degree 2 such that $f(A) \equiv 0 \mod 9$. Hence μ_A is a (3^ℓ)-minimal polynomial and $\{0,1,\ell\}$ is the ℓ-th index set of A (w.r.t. 3) for $\ell \geq 2$, and Theorem 2.3.15 implies

$$\mathsf{N}_3(A) = (X-1)(X-2)\,\mathbb{Z}[X] + 3\,\mathbb{Z}[X]$$

and

$$\forall\, \ell \geq 2: \ \ \mathsf{N}_{3^\ell}(A) = \mu_A\mathbb{Z}[X] + 3^{\ell-1}(X-1)(X-2)\,\mathbb{Z}[X] + 3^\ell\,\mathbb{Z}[X]$$

It remains to consider the case $p = 2$: Let $f = X \in \mathbb{Z}[X]$. Then $f(A) \equiv 0 \mod 2^\ell$ for $\ell \in \{1,2\}$. Hence f is a (2)- and a (4)-minimal polynomial of A. Therefore $\{0,\ell\}$ is the ℓ-th index set of A (w.r.t. 2) for $\ell \in \{1,2\}$ and, by Theorem 2.3.15,

$$\begin{aligned} \mathsf{N}_2(A) &= X\,\mathbb{Z}[X] + 2\,\mathbb{Z}[X] \\ \mathsf{N}_4(A) &= X\,\mathbb{Z}[X] + 4\,\mathbb{Z}[X] \end{aligned}$$

For $\ell \geq 3$, one observes, that there are at least two different entries on the diagonal of $[A]_{2^\ell}$ and therefore no monic, linear polynomial maps $[A]_{2^\ell}$ to the zero matrix.
However, it is easily seen that X^2 maps $[A]_8$ and $[A]_{16}$ to zero over ${}^{\mathbb{Z}}\!/\!_{8\mathbb{Z}}$ and ${}^{\mathbb{Z}}\!/\!_{16\mathbb{Z}}$, respectively, and therefore is a (8)- and (16)-minimal polynomial of A. Hence $\{0,2,\ell\}$ is the ℓ-th index set of A (w.r.t. 2) for $\ell \in \{3,4\}$ and Theorem 2.3.15 implies

$$\begin{aligned} \mathsf{N}_8(A) &= X^2\,\mathbb{Z}[X] + 2X\,\mathbb{Z}[X] + 8\,\mathbb{Z}[X] \text{ and} \\ \mathsf{N}_{16}(A) &= X^2\,\mathbb{Z}[X] + 4X\,\mathbb{Z}[X] + 16\,\mathbb{Z}[X] \end{aligned}$$

Now let $\ell = 5$. Then $[A]_{32}$ has three, pairwise different entries on the diagonal. Nevertheless, there exists a quadratic polynomial f such that $f(A) \equiv 0 \mod 32$, that is,

$f = X^2 + 4X$. Hence f is a (32)-minimal polynomial of A, $\{0, 2, 5\}$ is the fifth index set of A (w.r.t. 2) and, by Theorem 2.3.15,

$$\mathsf{N}_{32}(A) = (X^2 + 4X)\,\mathbb{Z}[X] + 8X\,\mathbb{Z}[X] + 32\,\mathbb{Z}[X]$$

holds. However for $\ell \geq 6$, one can check that, no monic, quadratic polynomial maps $[A]_{2^\ell}$ to zero. Hence μ_A is a (2^ℓ)-minimal polynomial and $\{0, 2, 5, \ell\}$ is the ℓ-th index set of A (w.r.t. 2) for $\ell \geq 6$. It follows from Theorem 2.3.15 that

$$\forall\, \ell \geq 6: \;\; \mathsf{N}_{2^\ell}(A) = \mu_A\mathbb{Z}[X] + 2^{\ell-5}(X^2 + 4X)\,\mathbb{Z}[X] + 2^{\ell-2}X\,\mathbb{Z}[X] + 2^\ell\,\mathbb{Z}[X]$$

2.4 Module structure of ${}^{D}\!/\!{}_{p^\ell D}[A]$

Throughout this section we fix the prime power $p^\ell \in D$ and write R_ℓ for the residue class ring ${}^{D}\!/\!{}_{p^\ell D}$. Let $A \in \mathrm{M}_n(R_\ell)$ be a square matrix with null ideal

$$\mathcal{N} = \mathcal{N}_{R_\ell}(A) = \{f \in R_\ell[X] \mid f(A) = 0\}.$$

Let $A' \in \mathrm{M}_n(D)$ be a preimage of A under the projection modulo p^ℓ, that is, $[A']_{p^\ell} = A$ where $[\,.\,]_{p^\ell}$ denotes the residue class modulo p^ℓ. Then, according to Theorem 2.3.15,

$$\mathcal{N} = \{[f]_{p^\ell} \in R_\ell[X] \mid f \in \mathsf{N}_{p^\ell}(A')\} = \sum_{i \in \mathcal{I}_\ell \setminus \{0\}} [p]_{p^\ell}^{\ell-i}[\nu_i]_{p^\ell} R_\ell[X]$$

where $\mathcal{I}_\ell$ is the ℓ-th index set of A' and ν_i are (p^i)-minimal polynomials of A' (for $i \in \mathcal{I}_\ell \setminus \{0\}$).

Notation and Conventions 2.4.1. Let $f' \in D[X]$ be a monic polynomial. Recall that, for $1 \leq j \leq \ell$, f' is a (p^j)-minimal polynomial of A' if and only if $f = [f']_{p^\ell}$ is a $([p^j]_{p^\ell})$-minimal polynomial of A, see Remark 2.3.3.
For a better readability, we often write p for the residue class $[p]_{p^\ell}$ of p modulo p^ℓ and say that $f \in R_\ell[X]$ is a (p^j)-minimal polynomial of A if it is a $([p^j]_{p^\ell})$-minimal polynomial of A.

Note that the ℓ-th index set of a matrix $A' \in \mathrm{M}_n(D)$ only depends on the residue class of A modulo p^ℓ, that is, if $A'' \in \mathrm{M}_n(D)$ is a matrix with $[A']_{p^\ell} = [A'']_{p^\ell}$ (and therefore $[A']_{p^j} = [A'']_{p^j}$ for all $1 \leq j \leq \ell$), then A' and A'' have equal ℓ-th index sets, cf. Remark 2.3.13.

Definition 2.4.2. Let $A \in \mathrm{M}_n(R_\ell)$ and $A' \in \mathrm{M}_n(D)$ such that $A = [A']_{p^\ell}$. If $\mathcal{I}_\ell$ is the ℓ-th index set of A', then we call $\mathcal{I}_\ell^\star = \mathcal{I}_\ell \setminus \{0, \ell\}$ the *reduced index set of* A. Further, for $i \in \mathcal{I}_\ell \setminus \{\ell\}$, we call $\mathrm{succ}(i) = \min\{i' \in \mathcal{I}_\ell \mid i' > i\}$ the *successor of* i *in* $\mathcal{I}_\ell$.

Remark 2.4.3. Let $A \in \mathrm{M}_n(R_\ell)$ with reduced index set $\mathcal{I}_\ell^\star$, and let $\nu_i \in R_\ell[X]$ be (p^j)-minimal polynomials of A (for $1 \leq i \leq \ell$). Then $i \in \mathcal{I}_\ell^\star$ if and only if $\deg(\nu_i) < \deg(\nu_{i+1})$, cf. Definition 2.3.12. Further, note that if $i \in \mathcal{I}_\ell^\star$, then $\deg(\nu_{\mathrm{succ}(i)}) = \deg(\nu_{i+1})$.

In this section we analyze the structure of the R_ℓ-module $R_\ell[A]$. Since the null ideal of A contains a monic polynomial, there exists a power of A which can be written as an R_ℓ-linear combination of smaller powers of A. Therefore the module $R_\ell[A]$ is finitely generated. As a finitely generated module over a principal ideal ring, $R_\ell[A]$ decomposes into cyclic R_ℓ-submodules, according to [2, Theorem 15.33]. We compute such a decomposition explicitly and demonstrate its relationship to the generating set of $\mathcal{N}(A)$ which we determined in Theorem 2.3.15 of the last section. In particular, it turns out that the invariant factors of $R_\ell[A]$ correspond to the elements in the reduced index set $\mathcal{I}_\ell^\star$ of A. Further, their multiplicities relate to the degrees of the (p^j)-minimal polynomials, see Remark 2.4.6. As the invariant factors are uniquely determined, this corroborates the usefulness of the set of generators of the null ideal of A which we determined in Section 2.3. To be more specific, Theorem 2.4.5 below states that, if $\mathcal{I}_\ell^\star$ is the reduced index set of A and $s_j = \deg(\nu_{\operatorname{succ}(j)}) - \deg(\nu_j)$ for $j \in \mathcal{I}_\ell^\star$, then

$$R_\ell[A] \simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{j \in \mathcal{I}_\ell^\star} (R_{\ell-j})^{s_j}. \tag{2.4.1}$$

where $\mathsf{d}_p = \deg(\nu_1)$ is the degree of the minimal polynomial of A modulo p. Roughly spoken, the R_ℓ-free part $R_\ell^{\mathsf{d}_p}$ of the decomposition in (2.4.1) indicates what happens in terms of classical linear algebra over the field R_1 while the torsion-part of $R_\ell[A]$ relates to the set $\mathcal{I}_\ell^\star$.

In order to understand this connection, let d be the degree of a (p^ℓ)-minimal polynomial ν_ℓ. Then A^d is an R_ℓ-linear combination of I, A, ..., A^{d-1}, and thus $R_\ell[A] = \left\langle I, A, \dots, A^{d-1} \right\rangle_{R_\ell}$. Hence the following sequence of R_ℓ-modules is exact.

$$\begin{array}{ccccccccc} \mathbf{0} & \longrightarrow & \ker(\psi) & \longrightarrow & R_\ell^d & \xrightarrow{\psi} & R_\ell[A] & \longrightarrow & \mathbf{0} \\ & & & & \mathbf{e}_i & \longmapsto & A^{i-1} & & \end{array} \tag{2.4.2}$$

where $\mathbf{e}_1$, …, $\mathbf{e}_d$ is an arbitrary basis of R_ℓ^d. It follows that

$$R_\ell[A] \simeq R_\ell^d / \ker(\psi).$$

Elements of $\ker(\psi)$ correspond to relations between the matrices I, A, …, A^{d-1} and therefore to polynomials in the null ideal $\mathcal{N}$ of A of degree less than d. Hence

$$\sum_{i=1}^{d} \lambda_i \mathbf{e}_i \in \ker(\psi) \quad \Longleftrightarrow \quad \sum_{i=1}^{d} \lambda_i X^{i-1} \in \mathcal{N} \tag{2.4.3}$$

where $\lambda_1, \dots, \lambda_d \in R_\ell$. We exploit this equivalence and use a generating set of the null ideal $\mathcal{N}$ of A to compute a generating set of the module $\ker(\psi)$. Nevertheless we need to be careful, since, as an ideal of $R_\ell[X]$, $\mathcal{N}$ is an $R_\ell[X]$-module and $\ker(\psi)$ is only an R_ℓ-module. Hence multiplication by X needs to be dealt with when transferring a generating set of $\mathcal{N}$ to a generating set of $\ker(\psi)$. For this purpose, set $R_\ell[X]^{<d} = \{f \in$

$R_\ell[X] \mid \deg(f) < d\}$. Then

$$\begin{aligned} \varphi : R_\ell[X]^{<d} &\overset{\sim}{\longrightarrow} R_\ell^d \\ X^{i-1} &\longmapsto \mathbf{e}_i \end{aligned} \tag{2.4.4}$$

is an R_ℓ-module isomorphism. Let

$$\mathcal{N}^{<d} = \{f \in \mathcal{N} \mid \deg(f) < d\}$$

be the set of all elements in $\mathcal{N}$ of degree less than d. Then $\mathcal{N}^{<d}$ is an R_ℓ-module, and for $f_1, \ldots, f_r \in R_\ell[X]^{<d}$, the following holds

$$\mathcal{N}^{<d} = \langle f_1, \ldots, f_r \rangle_{R_\ell} \quad \Longleftrightarrow \quad \ker(\psi) = \langle \varphi(f_1), \ldots, \varphi(f_r) \rangle_{R_\ell}$$

according to the equivalence in (2.4.3). We modify the sequence in (2.4.2) accordingly to get the following exact sequence of R_ℓ-modules.

$$\begin{aligned} \mathbf{0} \longrightarrow \mathcal{N}^{<d} \longrightarrow R_\ell[X]^{<d} &\longrightarrow R_\ell[A] \longrightarrow \mathbf{0} \\ X^i &\longmapsto A^i \end{aligned} \tag{2.4.5}$$

The following lemma describes which $R_\ell[X]$-generating sets of $\mathcal{N}$ can be transferred to R_ℓ-generating sets of $\mathcal{N}^{<d}$.

Lemma 2.4.4. *Let $A \in \mathrm{M}_n(R_\ell)$ be a square matrix over R_ℓ and d the degree of a (p^ℓ)-minimal polynomial of A. Further, let $f_1, \ldots, f_m$ be a generating set of the null ideal $\mathcal{N}$ of A in $R_\ell[X]$ such that*

1. $\deg(f_1) < \cdots < \deg(f_m) = d$,
2. *$f_i = [p^{t_i}]_{p^\ell} g_i$ for monic polynomials $g_i \in R_\ell[X]$ $(1 \le i \le m)$ and natural numbers $t_1 > \cdots > t_m$,*
3. *$f \in \sum_{i \in \mathcal{I}^{[f]}} f_i\, R_\ell[X]$ for all $f \in \mathcal{N}$, where $\mathcal{I}^{[f]} = \{1 \le i \le m \mid \deg(f_i) \le \deg(f)\}$.*

Then

$$\mathcal{N}^{<d} = \sum_{i=1}^{m-1} \sum_{t=1}^{s_i} (X^{t-1} f_i)\, R_\ell$$

where $s_i = \deg(f_{i+1}) - \deg(f_i)$.

Proof. Due to the conditions on the degrees of the polynomials f_i, it follows that $\deg(X^{t-1} f_i) < d$ for $1 \le i \le m-1$ and $1 \le t \le s_i$. Hence the inclusion "$\supseteq$" is easily seen and it suffices to show "$\subseteq$". Let $f \in \mathcal{N}^{<d}$. We prove this by induction on $\deg(f)$.

For the basis, let $0 \ne f \in \mathcal{N}^{<d}$ be a polynomial of minimal degree in $\mathcal{N}^{<d}$, that is, $\deg(f) \le \deg(g)$ for all $g \in \mathcal{N}^{<d}$. Since

$$f \in \sum_{i \in \mathcal{I}^{[f]}} f_i\, R_\ell[X]$$

it follows that $\mathcal{I}^{[f]} = \{1 \leq i \leq m \mid \deg(f_i) \leq \deg(f)\} \neq \emptyset$. Therefore $\deg(f) = \deg(f_1)$ and $\mathcal{I}^{[f]} = \{1\}$ (since $\deg(f_j) > \deg(f_1)$ for $j > 1$). Hence $f = rf_1$ for $r \in R_\ell$ which proves the basis.

Assume now $f \in \mathcal{N}^{<d}$ with $\deg(f) > \deg(f_1)$. Let $1 \leq k < m$ such that $\deg(f_k) \leq \deg(f) < \deg(f_{k+1})$. Then, $f \in \sum_{i=1}^{k} f_i R_\ell[X] \subseteq p^{t_k} R_\ell[X]$ according to our assumptions on the polynomials f_i (where we write p for its residue class $[p]_{p^\ell}$). Let $f' \in R_\ell[X]$ (with $\deg(f) = \deg(f')$) such that $f = p^{t_k} f'$. Since $f_k = p^{t_k} g_k$ for a monic polynomial $g_k \in R_\ell[X]$, there exist $q, r \in R_\ell[X]$ with $\deg(r) < \deg(g_k) = \deg(f_k)$ such that

$$f' = qg_k + r. \tag{2.4.6}$$

Therefore

$$f = qf_k + p^{t_k} r$$

which implies $p^{t_k}\, r \in \mathcal{N}^{<d}$, and we can apply the induction hypothesis. Hence

$$p^{t_k}\, r \in \sum_{i=1}^{m-1} \sum_{t=1}^{s_i} (X^{t-1} f_i)\, R_\ell$$

Since $\deg(f') = \deg(f) < \deg(f_{k+1})$, Equation (2.4.6) implies $\deg(q) = \deg(f) - \deg(f_k) < \deg(f_{k+1}) - \deg(f_k) = s_k$. Therefore

$$qf_k \in \sum_{t=1}^{s_k} (X^{t-1} f_k) R_\ell$$

and the assertion follows for $f = qf_k + p^{t_k}\, r$. □

According to Corollary 2.3.17, any generating set of the form $\{p^{\ell-i}\nu_i \mid i \in \mathcal{I}_\ell^\star\}$, where $\nu_i \in R_\ell[X]$ are (p^i)-minimal polynomials, satisfies the conditions of Lemma 2.4.4. This allows us to prove the following theorem which is the main result of this section.

Theorem 2.4.5. *Let $A \in \mathrm{M}_n(R_\ell)$ and $\nu_i \in R_\ell[X]$ be (p^i)-minimal polynomials with $d_i = \deg(\nu_i)$ for $0 \leq i \leq \ell$. Then*

$$R_\ell[A] \simeq \bigoplus_{i=0}^{\ell-1} (R_{\ell-i})^{d_{i+1}-d_i}$$

Further, let $\mathcal{I}_\ell^\star$ be the reduced index set of A and $s_i = \deg(\nu_{\mathrm{succ}(i)}) - \deg(\nu_i)$ for $i \in \mathcal{I}_\ell^\star$, then

$$R_\ell[A] \simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{i \in \mathcal{I}_\ell^\star} (R_{\ell-i})^{s_i}$$

where $\mathsf{d}_p = \deg(\nu_1)$ is the p-degree of A.

Proof. First, we show that the two decompositions of $R_\ell[A]$ given in the theorem, are isomorphic. Recall that $\nu_0 = 1$ and $d_0 = 0$. Hence $R_\ell^{\mathsf{d}_p} = R_{\ell-i}^{d_{i+1}-d_i}$ for $i = 0$. Let now $i \geq 1$. By Remark 2.4.3, an element $1 \leq i < \ell$ is in the reduced index set $\mathcal{I}_\ell^\star$ of A if and only if $d_i < d_{i+1}$, and if one of these equivalent conditions is satisfied, then $d_{i+1} = d_{\mathrm{succ}(i)}$. Therefore, $i \in \mathcal{I}_\ell^\star$ if and only if $R_{\ell-i}^{d_{i+1}-d_i} \neq \mathbf{0}$ and then $(R_{\ell-i})^{s_i} = (R_{\ell-i})^{d_{i+1}-d_i}$. Hence the two representations are isomorphic and it suffices to show that

$$R_\ell[A] \simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{i \in \mathcal{I}_\ell^\star} (R_{\ell-i})^{s_i}$$

According to Corollary 2.3.17 the polynomials in $\{p^{\ell-j}\nu_j \mid j \in \mathcal{I}_\ell^\star\}$ satisfy the conditions of Lemma 2.4.4, and therefore

$$\mathcal{N}^{<d} = \sum_{j \in \mathcal{I}_\ell^\star} \sum_{t=1}^{s_j} (p^{\ell-j} X^{t-1} \nu_j)\, R_\ell$$

Since $s_i = \deg(\nu_{\mathrm{succ}(i)}) - \deg(\nu_i)$, it follows that

$$\begin{array}{rccc} \delta : \{(i,t) \mid i \in \mathcal{I}_\ell^\star, 1 \leq t \leq s_i\} & \overset{\sim}{\longrightarrow} & \{\mathsf{d}_p + 1, \ldots, d\} \\ (i,t) & \longmapsto & \deg(\nu_i) + t \end{array}$$

is a bijection. For $1 \leq j \leq d$, we define

$$\mathbf{b}_j = \begin{cases} X^{j-1} & \text{if } 1 \leq j \leq \mathsf{d}_p \\ X^{t-1}\nu_i & \text{if } \mathsf{d}_p + 1 \leq j = \delta(i,t) \leq d \end{cases}$$

Observe that $\deg(\mathbf{b}_j) = j - 1$. Hence $\mathbf{b}_1, \ldots, \mathbf{b}_d$ is a basis of $R_\ell[X]^{<d}$. Together with the exact sequence (2.4.5), this implies

$$\begin{aligned} R_\ell[A] &\simeq {}^{R_\ell[X]^{<d}}/_{\mathcal{N}^{<d}} \\ &\simeq \bigoplus_{i=1}^{\mathsf{d}_p} \mathbf{b}_i\, R_\ell \oplus \bigoplus_{i \in \mathcal{I}_\ell^\star} \bigoplus_{t=1}^{s_i} {}^{\mathbf{b}_{\delta(i,t)} R_\ell}/_{(p^{\ell-i}\, \mathbf{b}_{\delta(i,t)}) R_\ell} \\ &\simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{i \in \mathcal{I}_\ell^\star} (R_{\ell-i})^{s_i} \end{aligned}$$

□

Remark 2.4.6. Let the notation be as in Theorem 2.4.5. If $\mathcal{I}_\ell^\star = \{i_1, \ldots, i_r\}$ with $i_1 < \cdots < i_r < i_{r+1} = \ell$. Then $s_{i_j} = \deg(\nu_{i_{j+1}}) - \deg(\nu_{i_j})$ for $1 \leq j \leq r$. According to Theorem 2.4.5, the uniquely determined invariant factors of $R_\ell[A]$ (with multiplicities) are

$$\underbrace{1, \ldots, 1}_{\mathsf{d}_p}, \underbrace{p^{\ell-i_1}, \ldots, p^{\ell-i_1}}_{s_{i_1}}, \ldots, \underbrace{p^{\ell-i_r}, \ldots, p^{\ell-i_r}}_{s_{i_r}}$$

Note that the occurring exponents $\ell - i_1, \dots, \ell - i_r$ of the invariant factors correspond to the elements of the set $\mathcal{I}_\ell^\star$. Further if $\nu_k \in R_\ell[X]$ is a (p^k)-minimal polynomial of A (for $1 \leq k \leq \ell$), then there exists $1 \leq u \leq r+1$ such that $\deg(\nu_k) = \deg(\nu_{i_u})$ and

$$\deg(\nu_k) = \sum_{i=0}^{k-1}(d_{i+1} - d_i) = \mathsf{d}_p + \sum_{j=1}^{u-1} s_{i_j}$$

Recall that the ℓ-th index set of a matrix defines a generating set of $\mathcal{N}_{R_\ell}(A)$ consisting of polynomials of the form $p^{\ell-j}\nu_j$. Per definition, $\mathcal{I}_\ell^\star$ depends on the degrees of these polynomials. In particular, observe that $\mathcal{I}_\ell^\star = \emptyset$ if and only if $\deg(\nu_\ell) = \deg(\nu_1) = \mathsf{d}_p$. Together with Theorems 2.3.15 and 2.4.5 this implies the following corollary.

Corollary 2.4.7. *Let $A \in \mathrm{M}_n(R_\ell)$ with ℓ-th index set $\mathcal{I}_\ell$, (p^ℓ)-minimal polynomial ν_ℓ and p-degree d_p. Then the following assertions are equivalent:*

1. $R_\ell[A] \simeq R_\ell^{\mathsf{d}_p}$
2. $\deg(\nu_\ell) = \mathsf{d}_p$
3. $\mathcal{N}_{R_\ell}(A) = \nu_\ell R_\ell[X]$

We can reformulate this in terms of matrices with entries in D.

Corollary 2.4.8. *Let $A \in \mathrm{M}_n(D)$ and $\ell \in \mathbb{N}$. Further let $\nu_j \in D[X]$ be (p^j)-minimal polynomials of A for $1 \leq j \leq \ell$ and $[A]_{p^j}$ be the image of A under the projection modulo p^j. The following assertions are equivalent.*

1. $\mathsf{N}_{p^\ell}(A) = \nu_\ell D[X] + p^\ell D[X]$.
2. $\mathsf{N}_{p^j}(A) = \nu_j D[X] + p^j D[X]$ *for all* $1 \leq j \leq \ell$.
3. $R_j[[A]_{p^j}] \simeq R_j^{\mathsf{d}_p}$ *for all* $1 \leq j \leq \ell$.
4. $\deg(\nu_\ell) = \mathsf{d}_p$.
5. ν_ℓ *is a* (p^j)*-minimal polynomial of* A *for all* $1 \leq j \leq \ell$.

Recall, that Proposition 2.3.18 states, that for $A \in \mathrm{M}_n(D)$, there exists $m \in \mathbb{N}$ such that $\deg(\nu_{m+k}) = \deg(\nu_A)$ for all $k \geq 0$. Then $\mathcal{I}_{m+k}^\star = \mathcal{I}_m^\star$, cf. Remark 2.3.14. Together with Theorem 2.4.5 we conclude this section with a final corollary.

Corollary 2.4.9. *Let $A \in \mathrm{M}_n(D)$ and ν_j be (p^j)-minimal polynomials for $j \geq 1$. Further, let $[A]_{p^j}$ be the image of A under the projection modulo p^j. Then there exists $m \in \mathbb{N}$ such that for all $\ell \geq m$ the following holds*

$$R_\ell[[A]_{p^\ell}] \simeq R_\ell^{\mathsf{d}_p} \oplus \bigoplus_{j \in \mathcal{I}_m^\star} (R_{\ell-j})^{s_j}$$

where $\mathcal{I}_m^\star$ is the reduced index set of $[A]_{p^m}$ and $s_j = \deg(\nu_{\mathrm{succ}(j)}) - \deg(\nu_j)$ for $j \in \mathcal{I}_m^\star$. In particular, $R_\ell[[A]_{p^\ell}]$ decomposes into $\deg(\mu_A)$ non-zero cyclic summands.

2.5 Integer-valued polynomials on one matrix

This section is dedicated to the application of the results of Section 2.3 in the context of integer-valued polynomials on a single matrix. Again, let D be a principal ideal domain with quotient field K and $A \in \mathrm{M}_n(D)$ a square matrix with entries in D. We want to determine the ring $\mathrm{Int}(A, \mathrm{M}_n(D))$ of all integer-valued polynomials on A, that is,

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \{f \in K[X] \mid f(A) \in \mathrm{M}_n(D)\}$$

Once we have an explicit description of $\mathrm{Int}(A, \mathrm{M}_n(D))$, we can determine the ring of images of A under $\mathrm{Int}(A, \mathrm{M}_n(D))$, that is,

$$\mathrm{Int}(A, \mathrm{M}_n(D))(A) = \{f(A) \mid f \in \mathrm{Int}(A, \mathrm{M}_n(D))\}$$

Let $f = \frac{g}{d} \in K[X]$ with $g \in D[X]$ and $d \in D$ and $d = \prod_{i=1}^{m} p_i^{\ell_i}$ the prime factorization of d. Then the following assertions are equivalent:

1. $f \in \mathrm{Int}(A, \mathrm{M}_n(D))$
2. $g(A) \equiv 0 \mod d\,\mathrm{M}_n(D)$
3. $g(A) \equiv 0 \mod p_i^{\ell_i}\,\mathrm{M}_n(D)$ for all $1 \leq i \leq m$

The results of Section 2.3 provide the tools to give an explicit description of the ring $\mathrm{Int}(A, \mathrm{M}_n(D))$ of integer-valued polynomials on A.

Theorem 2.5.1. *Let D be a principal ideal domain and $A \in \mathrm{M}_n(D)$ with minimal polynomial $\mu_A \in D[X]$. Then there exists a finite set $\mathcal{P}_A \subset \mathbb{P}$ of prime elements of D and natural numbers $m_p \in \mathbb{N}$ for $p \in \mathcal{P}_A$ such that*

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \mu_A K[X] + D[X] + \sum_{p \in \mathcal{P}_A} \sum_{j \in \mathcal{I}_{(p,m_p)}} \frac{\nu_{(p,j)}}{p^j} D[X]$$

where $\nu_{(p,j)} \in D[X]$ are (p^j)-minimal polynomials of A for $j \geq 1$, and $\mathcal{I}_{(p,m_p)}$ is the m_p-th index set of A w.r.t. the prime p.

Proof. It suffices to show "$\subseteq$". Recall that $\mathsf{N}_d(A) = \{f \in D[X] \mid f(A) \in d\,\mathrm{M}_n(D)\}$. Note that $\mathsf{N}_0(A) = \mathcal{N}_D(A) = \mu_A D[X] \subseteq D[X] = \mathsf{N}_1(A)$ and hence

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \sum_{d \in D \setminus \{0\}} \frac{1}{d} \mathsf{N}_d(A)$$

According to Lemma 2.3.5, this implies

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \sum_{p \in \mathbb{P}} \sum_{\ell \in \mathbb{N}} \frac{1}{p^\ell} \mathsf{N}_{p^\ell}(A) \tag{2.5.1}$$

First, we show that there exists a finite subset $\mathcal{P}_A \subseteq \mathbb{P}$ such that the following holds

$$\forall\, p \in \mathbb{P} \setminus \mathcal{P}_A : \ \mathsf{N}_{p^\ell}(A) = \mu_A D[X] + p^\ell D[X] \tag{2.5.2}$$

Considered as a matrix over K, A is similar to its rational canonical form C, cf. [23]. Let $\mu_1 \,|\, \dots \,|\, \mu_r = \mu_A$ be the invariant factors of A. Then there exists a matrix $T \in \mathrm{GL}_n(K)$ such that

$$T^{-1}AT = C = \mathcal{C}_{\mu_A} \oplus \cdots \oplus \mathcal{C}_{\mu_1}$$

where $\mathcal{C}_f$ denotes the companion matrix of a monic polynomial f. Since D is a principal ideal domain, it is integrally closed. As mentioned above, this implies $\mu_A \in D[X]$. Indeed, this implies that $\mu_i \in D[X]$ for all $1 \le i \le r$, since they are all monic divisors of the characteristic polynomial $\chi_A \in D[X]$, cf. [1, Ch. 5, §1.3, Prop. 11]. Therefore the rational canonical form C of A is a matrix with entries in D.
However, in general, A is not similar to C over the domain D, that is, we cannot assume $T \in \mathrm{GL}_n(D)$. Let $\mathcal{P}_A \subseteq \mathbb{P}$ be the set of prime elements which occur as divisors of the denominators of the entries of T or its inverse T^{-1}. Then $\mathcal{P}_A$ is finite and T, T^{-1} are invertible matrices over the localization $D_{(p)}$ of D at p for all $p \in \mathbb{P} \setminus \mathcal{P}_A$ and we can reduce the equation above modulo all $p \in \mathbb{P} \setminus \mathcal{P}_A$:

$$[T]_p^{-1}[A]_p[T]_p = [T^{-1}AT]_p = [C]_p = \mathcal{C}_{[\mu_A]_p} \oplus \cdots \oplus \mathcal{C}_{[\mu_1]_p}$$

(where we identify the residue fields of D and $D_{(p)}$ modulo p). It is well known, that a monic polynomial f is the minimal polynomial of its companion matrix $\mathcal{C}_f$ over any domain. Therefore $[\mu_A]_p$ is the minimal polynomial of $\mathcal{C}_{[\mu_A]_p}$. Further, $[\mu_A]_p(\mathcal{C}_{[\mu_i]_p}) = 0$ holds since $\mu_i \,|\, \mu_A$ for all $1 \le i \le m$. Hence μ_A is a (p)-minimal polynomial for all $p \in \mathbb{P} \setminus \mathcal{P}_A$, which implies the assertion in (2.5.2) above, according to Corollary 2.4.8.
Thus, Equations (2.5.1) and (2.5.2) imply

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \mu_A K[X] + D[X] + \sum_{p \in \mathcal{P}_A} \sum_{\ell \ge 1} \frac{1}{p^\ell} \mathsf{N}_{p^\ell}(A) \tag{2.5.3}$$

Further, by Corollary 2.3.19, for all prime elements $p \in \mathcal{P}_A$, there exists $m_p \in \mathbb{N}$ such that for all $\ell \ge m_p$

$$\mathsf{N}_{p^\ell}(A) = \mu_A D[X] + p^{\ell - m_p} \mathsf{N}_{p^{m_p}}(A)$$

holds, and we can restrict the inner sum in Equation (2.5.3) to all $1 \le \ell \le m_p$. And finally, since $p\mathsf{N}_{p^{\ell-1}}(A) \subseteq \mathsf{N}_{p^\ell}(A)$, it follows hat $\frac{1}{p^{\ell-1}}\mathsf{N}_{p^{\ell-1}}(A) \subseteq \frac{1}{p^\ell}\mathsf{N}_{p^\ell}(A)$. Hence

$$\sum_{\ell=1}^{m_p} \frac{1}{p^\ell} \mathsf{N}_{p^\ell}(A) = \frac{1}{p^{m_p}} \mathsf{N}_{p^{m_p}}(A)$$

Then, Theorem 2.3.15 implies

$$\mathrm{Int}(A, \mathrm{M}_n(D)) = \mu_A K[X] + D[X] + \sum_{p \in \mathcal{P}_A} \sum_{j \in \mathcal{I}_{(p,m_p)}} \frac{\nu_{(p,j)}}{p^j} D[X]$$

□

Corollary 2.5.2. *Let D be a principal ideal domain and $A \in \mathrm{M}_n(D)$ with minimal polynomial $\mu_A \in D[X]$. Then there exists a finite set $\mathcal{P}_A \subset \mathbb{P}$ and natural numbers $m_p \in \mathbb{N}$ for $p \in \mathcal{P}_A$ such that*

$$\mathrm{Int}(A, \mathrm{M}_n(D))(A) = D[A] + \sum_{p \in \mathcal{P}_A} \sum_{j \in \mathcal{I}_{(p,m_p)}} \frac{\nu_{(p,j)}(A)}{p^j} D[A]$$

where $\nu_{(p,j)} \in D[X]$ are (p^j)-minimal polynomial of A for $j \geq 1$, and $\mathcal{I}_{(p,m_p)}$ is the m_p-th index set of A w.r.t. the prime p.

Example 2.5.3. We continue Example 2.3.20, and determine the ring $\mathrm{Int}(A, \mathrm{M}_3(\mathbb{Z}))$ of integer-valued polynomials on A and the ring $\mathrm{Int}(A, \mathrm{M}_3(\mathbb{Z}))(A)$ of integer-valued images for

$$A = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 16 & 0 \\ 0 & 0 & 32 \end{pmatrix} \in \mathrm{M}_3(\mathbb{Z})$$

We know that

$$\mathrm{Int}(A, \mathrm{M}_3(\mathbb{Z})) = \sum_{p \in \mathbb{P}} \sum_{\ell \in \mathbb{N}} \frac{1}{p^\ell} \mathsf{N}_{p^\ell}(A).$$

According to Example 2.3.20, the following holds:

$$\forall\, p \in \mathbb{P} \setminus \{2, 3, 7\}\ \forall\, \ell \geq 1 : \quad \mathsf{N}_{p^\ell}(A) = \mu_A \mathbb{Z}[X] + p^\ell \mathbb{Z}[X]$$

and hence

$$\mathrm{Int}(A, \mathrm{M}_3(\mathbb{Z})) = \mu_A \mathbb{Q}[X] + D[X] + \sum_{\ell \in \mathbb{N}} (\frac{1}{2^\ell} \mathsf{N}_{2^\ell}(A) + \frac{1}{3^\ell} \mathsf{N}_{3^\ell}(A) + \frac{1}{7^\ell} \mathsf{N}_{7^\ell}(A)).$$

Further, Example 2.3.20 implies that for $\ell \geq 2$

$$\frac{1}{3^\ell} \mathsf{N}_{3^\ell}(A) = \frac{1}{3^\ell} \mu_A \mathbb{Z}[X] + \mathbb{Z}[X] + \frac{1}{3} \mathsf{N}_3(A)$$

Similarly, one can deduce that

$$\frac{1}{7^\ell} \mathsf{N}_{7^\ell}(A) = \frac{1}{7^\ell} \mu_A \mathbb{Z}[X] + \mathbb{Z}[X] + \frac{1}{7} \mathsf{N}_7(A)$$

holds for all $\ell \geq 2$. And finally, Example 2.3.20 implies that

$$\frac{1}{2^\ell} \mathsf{N}_{p^\ell}(A) = \frac{1}{2^\ell} \mu_A \mathbb{Z}[X] + \mathbb{Z}[X] + \frac{1}{32} \mathsf{N}_{32}(A)$$

for all $\ell \geq 6$. Since $\mathsf{N}_{32}(A) \supseteq 2^{5-j}\mathsf{N}_{2^j}(A)$ for $j \in \{1,2,3,4\}$, it follows that

$$\begin{aligned}\operatorname{Int}(A, \mathrm{M}_3(\mathbb{Z})) &= \mu_A\mathbb{Q}[X] + \mathbb{Z}[X] + \frac{1}{3}\,\mathsf{N}_3(A) + \frac{1}{7}\,\mathsf{N}_7(A) + \frac{1}{32}\,\mathsf{N}_{32}(A)\\ &= \mu_A\mathbb{Q}[X] + \mathbb{Z}[X] + \sum_{p\in\{2,3,5\}} \frac{1}{p^{m_p}}\,\mathsf{N}_{p^{m_p}}(A)\end{aligned}$$

where $m_2 = 5$ and $m_3 = m_7 = 1$. Hence

$$\begin{aligned}\operatorname{Int}(A, \mathrm{M}_3(\mathbb{Z})) =&(X-4)(X-16)(X-32)\mathbb{Q}[X] + \mathbb{Z}[X]\\ &+ \frac{1}{3}(X-1)(X-2)\mathbb{Z}[X] + \frac{1}{7}(X-2)(X-4)\mathbb{Z}[X]\\ &+ \frac{1}{32}(X^2+4X)\mathbb{Z}[X] + \frac{1}{4}X\mathbb{Z}[X]\end{aligned}$$

And finally, this implies

$$\begin{aligned}\operatorname{Int}(A, \mathrm{M}_3(\mathbb{Z}))(A) = \mathbb{Z}[A] &+ \begin{pmatrix}2 & 0 & 0\\ 0 & 70 & 0\\ 0 & 0 & 310\end{pmatrix}\mathbb{Z}[A] + \begin{pmatrix}0 & 0 & 0\\ 0 & 24 & 0\\ 0 & 0 & 120\end{pmatrix}\mathbb{Z}[A]\\ &+ \begin{pmatrix}1 & 0 & 0\\ 0 & 10 & 0\\ 0 & 0 & 36\end{pmatrix}\mathbb{Z}[A] + \begin{pmatrix}1 & 0 & 0\\ 0 & 4 & 0\\ 0 & 0 & 8\end{pmatrix}\mathbb{Z}[A]\end{aligned}$$

3 Finiteness and Skolem closure over non-unibranched domains

This chapter contains the article [8] with the title *Finiteness and Skolem closure of ideals for non-unibranched domains*. It is joint work with Paul-Jean Cahen. The article appeared in the journal *Communications in Algebra* (Vol. 43, Issue 6) in April 2015.

3.1 Abstract

A one-dimensional, Noetherian, local domain D with maximal ideal $\mathfrak{m}$ and finite residue field has been known to be an almost strong Skolem ring if analytically irreducible. It is unknown whether this condition is necessary. We show that it is at least necessary that D be unibranched. After introducing a general notion of equalizing ideal, we show that, for k large enough, the ideals of the form $\mathfrak{M}_{k,a} = \{f \in \mathrm{Int}(D) \mid f(a) \in \mathfrak{m}^k\}$, for $a \in D$, are distinct. This allows to show that the maximal ideals $\mathfrak{M}_a = \{f \in \mathrm{Int}(D) \mid f(a) \in \mathfrak{m}\}$, although not necessarily distinct, are never finitely generated.

Keywords. Integer-valued polynomials, Skolem properties, analytically irreducible domain, unibranched domain.

2000 Mathematics Subject Classification. 13F20

3.2 Introduction

The classical ring of integer-valued polynomials is the ring $\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$ of polynomials with rational coefficients taking integer values on the integers. This ring has many interesting properties. First of all, it is probably the simplest and most natural example of a non-Noetherian domain. Among other properties, Skolem [24] pointed out that, given finitely many integer-valued polynomials $g_1, \dots, g_k$ such that $g_1(n), \dots, g_k(n)$ are relatively prime for each integer n, the ideal generated by these polynomials in $\mathrm{Int}(\mathbb{Z})$ is the whole ring $\mathrm{Int}(\mathbb{Z})$ (while a similar property does not hold for polynomials with coefficients in $\mathbb{Z}$).

More generally, for a domain D with quotient field K, one can study the properties of the ring of integer-valued polynomials

$$\mathrm{Int}(D) = \{f \in K[X] \mid f(D) \subseteq D\}.$$

The reader is referred to [6] for a survey. We aim in this paper to answer some questions on the Noetherian and Skolem properties, that remained open from the time of publication of this survey. Usually, the main focus is on the case where D is Noetherian. In this case, $\mathrm{Int}(D)_{\mathfrak{p}} = \mathrm{Int}(D_{\mathfrak{p}})$ for every prime $\mathfrak{p}$ of D [6, Theorem I.2.3]. For most properties, one can thus assume D to be a local ring with maximal ideal $\mathfrak{m}$ (however the Skolem property does not localize, but we come back, in more details, to this question later on in this introduction). One can also assume that the residue field $D/\mathfrak{m}$ is finite, lest $\mathrm{Int}(D) = D[X]$ [6, Corollary I.3.7]. Finally, one can assume that the Krull dimension of D is one, otherwise one has the containment $D[X] \subseteq \mathrm{Int}(D) \subseteq D'[X]$, where D' denotes the integral closure of D [6, Corollary IV.4.10], a case that is not entirely trivial (unless D is integrally closed) but, in some sense, less interesting (for instance it may occur in this case that $\mathrm{Int}(D)$ is Noetherian).

The first question we address deals with the prime spectrum of $\mathrm{Int}(D)$ and the finiteness of some maximal ideals. In the case of a one-dimensional local domain D, there are two types of prime ideals: those above (0) and those above the maximal ideal $\mathfrak{m}$ of D. Let us focus on the second type (the first one is easily described, whatever the domain D is [6, Corollary V.1.2]). Recall that, given a maximal ideal $\mathfrak{m}$ of any domain D, we have for each $a \in D$ a prime ideal of $\mathrm{Int}(D)$ above $\mathfrak{m}$ of the form

$$\mathfrak{M}_a = \{f \in \mathrm{Int}(D) \mid f(a) \in \mathfrak{m}\}.$$

These primes are clearly maximal. In the case of a one-dimensional, Noetherian, local domain D with maximal ideal $\mathfrak{m}$, the polynomials with coefficients in K are continuous functions in the $\mathfrak{m}$-adic topology [6, Proposition III.2.1]. Considering the $\mathfrak{m}$-adic completion $\widehat{D}$ of D, we thus have also, for each $\alpha \in \widehat{D}$, maximal ideals of the form $\mathfrak{M}_\alpha = \{f \in \mathrm{Int}(D) \mid f(\alpha) \in \widehat{\mathfrak{m}}\}$ where $\widehat{\mathfrak{m}}$ is the topological closure of $\mathfrak{m}$ in $\widehat{D}$. If moreover the residue field $D/\mathfrak{m}$ is finite, all the prime ideals of $\mathrm{Int}(D)$ above $\mathfrak{m}$ are of the form $\mathfrak{M}_\alpha$ [6, Proposition V.2.2]. Yet these ideals are not necessarily distinct and it may happen that, in fact, they are all of the form $\mathfrak{M}_a$ for some $a \in D$. More precisely, as summarized in [6, Chapter V], if D is a discrete valuation domain, or more generally, if D is analytically irreducible, that is, $\widehat{D}$ is a domain, there is a one-to-one correspondence between the elements of $\widehat{D}$ and the prime ideals of $\mathrm{Int}(D)$ above $\mathfrak{m}$ (to $\alpha \in \widehat{D}$ corresponds $\mathfrak{M}_\alpha$). This nice property is linked with the Stone-Weierstrass theorem (if D is analytically irreducible, the ring of integer-valued polynomials is dense in the ring of continuous functions from $\widehat{D}$ to $\widehat{D}$). Under the weaker hypothesis that D is unibranched, that is, the integral closure D' of D is local, this is no longer the case but it remains at least true that the ideals $\mathfrak{M}_a$, for $a \in D$, are all distinct (one must consider the $\mathfrak{m}'$-adic completion of D, where $\mathfrak{m}'$ is the maximal ideal of D', rather than the $\mathfrak{m}$-adic completion, to obtain a one-to-one correspondence). Finally, in the non-unibranched case, there are only finitely many prime ideals of $\mathrm{Int}(D)$ above $\mathfrak{m}$, all of them of the form $\mathfrak{M}_a$ $(a \in D)$, these primes being in one-to-one correspondence with the residue classes of D modulo some nonzero ideal $\mathfrak{q}_{\mathfrak{m}}$ of D, called the equalizing ideal of $\mathfrak{m}$ in $\mathrm{Int}(D)$.

In case the ideals $\mathfrak{M}_a$ are all distinct, there is a very easy argument to show these ideals are not finitely generated: assume by way of contradiction that $\mathfrak{M}_a = (f_1, \ldots, f_n)$. Thus $f_i(a) \in \mathfrak{m}$ for all i and by continuity, $f_i(b) \in \mathfrak{m}$ for b close enough to a. Hence $f_1, \ldots, f_n$ are in $\mathfrak{M}_b$, and one would have $\mathfrak{M}_a \subseteq \mathfrak{M}_b$ in contradiction with the fact that the ideals $\mathfrak{M}_a$ are maximal and all distinct. This argument cannot be used if the ideals $\mathfrak{M}_a$ are

not distinct, that is, if D is not unibranched. However, we show in this paper that, unibranched or not unibranched, the ideals $\mathfrak{M}_a$ are never finitely generated.
The second question deals with the Skolem properties. If $\mathfrak{A}$ is an ideal of $\mathrm{Int}(D)$, then for each $a \in D$, the set $\mathfrak{A}(a) = \{f(a) \mid f \in \mathfrak{A}\}$ is clearly an ideal of D called the *ideal of values* of $\mathfrak{A}$ at a. The property pointed out by Skolem in the case of $\mathrm{Int}(\mathbb{Z})$ (the *Skolem property*) is that, given a finitely generated ideal $\mathfrak{A}$ of $\mathrm{Int}(D)$, if $\mathfrak{A}(a) = D$ for each $a \in D$, then $\mathfrak{A} = \mathrm{Int}(D)$. In fact, $\mathrm{Int}(\mathbb{Z})$ satisfies even a stronger property (the *strong Skolem property*): given two finitely generated ideals $\mathfrak{A}$ and $\mathfrak{B}$, if $\mathfrak{A}(a) = \mathfrak{B}(a)$ for each $a \in D$, then $\mathfrak{A} = \mathfrak{B}$. Now the Skolem property (let alone the strong Skolem property) cannot hold if D is a local ring: the polynomial $f = 1 + tX$ with $t \in \mathfrak{m}$ is clearly such that $f(a)$ is a unit for each $a \in D$, whereas the ideal generated by f is not the whole ring $\mathrm{Int}(D)$ (indeed, it fails to contain any nonzero constant). In fact, it turns out that, to study the Skolem properties, one can split the ideals of $\mathrm{Int}(D)$ into two categories: the ideals which contain nonzero constants, called the *unitary ideals*, and the ideals $\mathfrak{A}$ such that $\mathfrak{A} \cap D = (0)$ (in the case of a one-dimensional local ring with maximal ideal $\mathfrak{m}$, the prime ideals above $\mathfrak{m}$ are thus the unitary prime ideals). Finally, it is convenient to phrase the Skolem properties in terms of *Skolem closure*. The reader can find a survey in [6, Chapter VII]), and we summarize the needed definitions as follows:

Definition 3.2.1. Let $\mathfrak{A}$ be an ideal of $\mathrm{Int}(D)$, we call

$$\mathfrak{A}^{\star} = \{f \in \mathrm{Int}(D) \mid \forall a \in D : f(a) \in \mathfrak{A}(a)\}$$

the *Skolem closure* of $\mathfrak{A}$. We further say that $\mathfrak{A}$ is *Skolem closed*, if $\mathfrak{A} = \mathfrak{A}^{\star}$.

The Skolem closure of $\mathfrak{A}$ is the largest ideal $\mathfrak{B}$ of $\mathrm{Int}(D)$ such that $\mathfrak{A}$ and $\mathfrak{B}$ have the same ideals of values, that is, $\mathfrak{A}(a) = \mathfrak{B}(a)$ for each $a \in D$.

Definition 3.2.2.

1. We say that D is a *Skolem ring* (resp. an *almost Skolem ring*) or that $\mathrm{Int}(D)$ satisfies the *Skolem property* (resp. the *almost Skolem property*), if for each finitely generated ideal (resp. for each finitely generated unitary ideal) $\mathfrak{A}$ of $\mathrm{Int}(D)$, $\mathfrak{A}^{\star} = \mathrm{Int}(D)$ implies $\mathfrak{A} = \mathrm{Int}(D)$.

2. We say that D is a *strong Skolem ring* (resp. an *almost strong Skolem ring*) or that $\mathrm{Int}(D)$ satisfies the *strong Skolem property* (resp. the *almost strong Skolem property*), if each finitely generated ideal (resp. finitely generated unitary ideal) $\mathfrak{A}$ of $\mathrm{Int}(D)$ is Skolem closed.

The "almost" properties are thus the Skolem properties restricted to the (finitely generated) unitary ideals. As for the non-unitary ideals, they are linked to a natural divisibility property [14]: D is said to be a *d-ring* if each integer-valued rational function on D is in fact an integer-valued polynomial (equivalently for each non-constant polynomial f with coefficients in D, there exists $a \in D$ such that $f(a)$ is not a unit in D, equivalently also, for each finitely generated non-unitary ideal $\mathfrak{A}$, there exists $a \in D$ with $\mathfrak{A}(a) \neq D$). Finally it turns out that a ring is a (strong) Skolem ring if and only if it is an almost (strong) Skolem d-ring [6, Proposition VII.2.14].

The almost (strong) Skolem property does localize and hence, to study this property in the Noetherian case, one may assume, as above, that D is a one-dimensional, Noetherian, local domain with finite residue field. Under these hypotheses, D is always an almost Skolem ring [6, Lemma VII.4.2] and this is because, as said above, all the prime ideals of Int(D) above $\mathfrak{m}$ are of the form $\mathfrak{M}_\alpha$ for some $\alpha \in \widehat{D}$. The almost strong Skolem property holds in case D is analytically irreducible [6, Corollary VII.3.9] and this, as for the first question considered here, thanks to the Stone-Weierstrass theorem. Yet, it was not known whether it is necessary that D is analytically irreducible to be an almost strong Skolem ring [6, Remark VII.3.10]. Our second result shows that D must at least be unibranched. (Recall that under our hypotheses D is analytically irreducible if and only if D it is unibranched and the integral closure D' is finitely generated as a D-module.) This result had been announced in a survey on Skolem properties [7] in 1999 but has not been proved since then.

To reach our goal, we generalize in the next section the notion of equalizing ideal, considering the equalizing ideal $\mathfrak{q}_I$ of an arbitrary ideal I of D. In the particular case where $I = \mathfrak{m}^k$ (for some integer k), we consider, for each $a \in D$ the ideals of Int(D) of the form

$$\mathfrak{M}_{k,a} = \{f \in \text{Int}(D) \mid f(a) \in \mathfrak{m}^k\}$$

and then have $\mathfrak{M}_{k,a} = \mathfrak{M}_{k,b}$ if and only if $a \equiv b \pmod{\mathfrak{q}_{\mathfrak{m}^k}}$. We show that for k large enough, $\mathfrak{q}_{\mathfrak{m}^k}$ is trivial, that is, $\mathfrak{q}_{\mathfrak{m}^k} = (0)$, equivalently we thus show that for k large enough, the ideals $\mathfrak{M}_{k,a}$ are distinct. This holds whether D is unibranched or not, but simply, if D is unibranched, it holds for each $k \geq 1$, whereas if D is not unibranched, one must take $k > 1$. This can be considered as the main result of this paper as we can then derive easily, in the next and final section, the two results we were aiming at.

For instance, it immediately follows that the ideals $\mathfrak{M}_{k,a}$ are not finitely generated with the same easy argument as for the ideals $\mathfrak{M}_a$ (as recalled above, in case D is unibranched). We could derive of course that Int(D) is not Noetherian (yet, this was already known for every one-dimensional, Noetherian domain D, unless Int(D) is trivial, that is, Int$(D) = D[X]$ [6, Corollary VI.2.6]). More interestingly, we can prove also that the quotient ring Int$(D)/\mathfrak{m}^k\,$Int(D) is not Noetherian (using the fact that the ideals $\mathfrak{M}_{k,a}/\mathfrak{m}^k\,Int(D)$ are not finitely generated) and finally can conclude that the ideals of the form $\mathfrak{M}_a$ are never finitely generated.

It is now also easy to prove that an almost strong Skolem ring must be unibranched. Indeed, in case there are only finitely many ideals of the form $\mathfrak{M}_a$ (that is, in case D is not unibranched), it is easy to produce a finitely generated ideal $\mathfrak{A}$ containing $\mathfrak{m}$ and contained in one and only one ideal of the form $\mathfrak{M}_a$. It follows that the ideals of values of $\mathfrak{A}$ and $\mathfrak{M}_a$ are the same (that is, $\mathfrak{A}(x) = \mathfrak{M}_a(x)$ for each $x \in D$). As $\mathfrak{M}_a$ is not finitely generated, there is obviously a finitely generated ideal $\mathfrak{B}$ such that $\mathfrak{A} \subsetneq \mathfrak{B} \subsetneq \mathfrak{M}_a$. Clearly, $\mathfrak{A}$ and $\mathfrak{B}$ must then have the same ideal of values, they are both finitely generated, they both contain $\mathfrak{m}$, thus are both unitary, but $\mathfrak{A} \neq \mathfrak{B}$. We can therefore conclude that D is not an almost strong Skolem ring.

3.3 Generalized equalizing ideals

In this section we generalize the notion of equalizing ideal. First, for an arbitrary ideal I of a domain D, we set

$$\mathfrak{I}_{I,a} = \{f \in \mathrm{Int}(D) \mid f(a) \in I\}.$$

Clearly, $\mathfrak{I}_{I,a}$ is the kernel of the map sending a polynomial $f \in \mathrm{Int}(D)$ on the class $\overline{f(a)}$ of $f(a)$ in the quotient ring D/I, and thus is an ideal of $\mathrm{Int}(D)$ above I (that is, $\mathfrak{I}_{I,a} \cap D = I$). The quotient $\mathrm{Int}(D)/\mathfrak{I}_{I,a}$ is thus isomorphic to D/I, hence $\mathfrak{I}_{I,a}$ is a prime ideal (resp. a maximal ideal) of $\mathrm{Int}(D)$ if and only if I is a prime ideal (resp. a maximal ideal) of D (as already observed, in a more general setting, in [6, Lemma V.1.3], for polynomials that are integer-valued on a subset of the domain D). Obviously, if $I = \mathfrak{m}$ is a maximal ideal, the ideals $\mathfrak{I}_{\mathfrak{m},a}$ are nothing else than the classical ideals $\mathfrak{M}_a$ described above. In the special case where $I = \mathfrak{m}^k$ we thus simply denote $\mathfrak{I}_{\mathfrak{m}^k,a}$ by $\mathfrak{M}_{k,a}$.
Raising the question whether the ideals of the form $\mathfrak{I}_{I,a}$ are distinct or not, we introduce the equalizing ideal of I similarly to the equalizing ideal $\mathfrak{q}_\mathfrak{m}$ of $\mathfrak{m}$, introduced by Cahen and Chabert in [6] as the set of elements $a \in D$ such that $\mathfrak{M}_a = \mathfrak{M}_0$. We rephrase this definition and follow the results of [6, Proposition V.3.5], in this more general setting, as follows.

Proposition 3.3.1. *Let I be an ideal of a domain D and consider the subset $\mathfrak{q}_I$ of D defined by*

$$\mathfrak{q}_I = \{a \in D \mid \forall f \in \mathrm{Int}(D) : f(a) - f(0) \in I\}.$$

Then

(*i*) *$a - b \in \mathfrak{q}_I$ if and only if, for all $f \in \mathrm{Int}(D)$, $f(a) - f(b) \in I$,*

(*ii*) *$\mathfrak{q}_I$ is an ideal of D,*

(*iii*) *$\mathfrak{q}_I \subseteq I$.*

Proof. (i) By definition, $a - b \in \mathfrak{q}_I$ if and only if, for all $f \in \mathrm{Int}(D)$, we have $f(a - b) - f(0) \in I$. Considering the isomorphism of $\mathrm{Int}(D)$ onto itself, sending f to the polynomial g such that $g(X) = f(X - b)$, we see that $f(a - b) - f(0) \in I$ (for all $f \in \mathrm{Int}(D)$) if and only $g(a) - g(b) \in I$ (for all $g \in \mathrm{Int}(D)$).
(ii) Let $a, b \in \mathfrak{q}_I$. By definition, for all $f \in \mathrm{Int}(D)$ we have $f(a) - f(0) \in I$ and $f(b) - f(0) \in I$, and thus $f(a) - f(b) \in I$. By (i) it follows that $a - b \in \mathfrak{q}_I$. Next, let $a \in \mathfrak{q}_I$ and $\lambda \in D$. Setting $h(X) = f(\lambda X)$, then $h \in \mathrm{Int}(D)$, and thus, $f(\lambda a) - f(0) = h(a) - h(0) \in I$. Therefore $\lambda a \in \mathfrak{q}_I$. We can conclude that $\mathfrak{q}_I$ is an ideal.
(iii) As $f = X$ belongs to $\mathrm{Int}(D)$, $a \in \mathfrak{q}_I$ implies $a = f(a) - f(0) \in I$. Thus $\mathfrak{q}_I \subseteq I$. □

With these notations we then set the following definition.

Definition 3.3.2. The ideal $\mathfrak{q}_I$ is called the *equalizing ideal* of I in $\mathrm{Int}(D)$.

The equalizing ideal (as its name suggests) allows to determine whether two ideals of the form $\mathfrak{I}_{I,a}$ are distinct or even whether they are comparable. Yet, as the ideals $\mathfrak{I}_{I,a}$ are not maximal in general (unless I is maximal), the containment $\mathfrak{I}_{I,a} \subseteq \mathfrak{I}_{I,b}$ does not imply a priori the equality $\mathfrak{I}_{I,a} = \mathfrak{I}_{I,b}$, contrary to the case of the ideals $\mathfrak{M}_a$. Nevertheless, this implication turns out to be true.

Corollary 3.3.3. *Let I be an ideal of the domain D and $\mathfrak{q}_I$ be the corresponding equalizing ideal. Then the following assertions are equivalent.*

(*i*) $\mathfrak{I}_{I,a} = \mathfrak{I}_{I,b}$,

(*ii*) $\mathfrak{I}_{I,a} \subseteq \mathfrak{I}_{I,b}$,

(*iii*) $a \equiv b \pmod{\mathfrak{q}_I}$.

Proof. That (i) implies (ii) is trivial.
Deny (iii), then $a - b \notin \mathfrak{q}_I$. By definition, there is a polynomial $f \in \mathrm{Int}(D)$ such that $f(a-b) - f(0) \notin I$. Set $g(X) = f(a - X) - f(0)$. Then $g \in \mathrm{Int}(D)$, $g(a) = 0$, and $g(b) = f(a - b) - f(0)$. Thus $g(a) \in I$, that is, $g \in \mathfrak{I}_{I,a}$, while $g(b) \notin I$, that is, $g \notin \mathfrak{I}_{I,b}$. Hence $\mathfrak{I}_{I,a} \not\subseteq \mathfrak{I}_{I,b}$. Therefore (ii) implies (iii).
Suppose (iii), that is, $a - b \in \mathfrak{q}_I$. It follows from the first assertion of Proposition 3.3.1, that, for all $f \in \mathrm{Int}(D)$, we have $f(a) - f(b) \in I$. Thus $f(a) \in I$ if and only if $f(b) \in I$, that is $\mathfrak{I}_{I,a} = \mathfrak{I}_{I,b}$. □

Another way to phrase Corollary 3.3.3 is to say there is a one-to-one correspondence between the ideals of the form $\mathfrak{I}_{I,a}$ and the residue classes of D modulo $\mathfrak{q}_I$. In particular, the ideals $\mathfrak{I}_{I,a}$ are all distinct if and only if the equalizing ideal is trivial, that is, $\mathfrak{q}_I = (0)$. Moreover, it is known that, for every nonzero ideal I of a one-dimensional, Noetherian, local domain with finite residue field, the residue ring D/I is finite. In this case, when the equalizing ideal is not trivial there are but finitely many ideals of the type $\mathfrak{I}_{I,a}$.
We next easily show that equalizing ideals preserve inclusion.

Proposition 3.3.4. *Let I, J be two ideals of the domain D such that $I \subseteq J$. Then $\mathfrak{q}_I \subseteq \mathfrak{q}_J$.*

Proof. Assume $a \notin \mathfrak{q}_J$: there exists $f \in \mathrm{Int}(D)$ such that $f(a) - f(0) \notin J$. A fortiori $f(a) - f(0) \notin I$, and hence $a \notin \mathfrak{q}_I$. □

To ensure that $\mathfrak{q}_I$ is trivial for some ideal I it is then enough to find a larger ideal J with a trivial equalizing ideal $\mathfrak{q}_J$. We shall use this argument below, but first consider some easy examples.

Remark 3.3.5. Given a D-algebra B such that $X \in B$, $B \subseteq K[X]$, and the property that, for each $f \in B$ and each $a \in D$, $f(a - X), f(X - a), f(aX) \in B$, we could more generally consider the ideals of the form $\mathfrak{I}_{I,a}$, for every ideal I of D, and the corresponding equalizing ideal $\mathfrak{q}_I$, with the same definitions and the same properties as for $\mathrm{Int}(D)$.
For instance, for $B = D[X]$ (the classical ring of polynomials with coefficients in D), we know that, for $f \in D[X]$ and $a, b \in D$, $a - b$ divides $f(a) - f(b)$ in D. It follows that, for

every ideal I, $a \in I$ implies $f(a) - f(0) \in I$, that is, $a \in \mathfrak{q}_I$. As $\mathfrak{q}_I$ is always contained in I, we then have $\mathfrak{q}_I = I$. In particular the equalizing ideal $\mathfrak{q}_I$ of every nonzero ideal I is not trivial and the ideals of the form $\mathfrak{I}_{I,a}$ are not all distinct (however that does not necessarily mean there are finitely many such ideals, since the residue ring D/I is not finite in general). The same may happen for $\operatorname{Int}(D)$ (let alone because it may happen that $\operatorname{Int}(D) = D[X]$).
On the opposite, for $B = \operatorname{Int}(D)$, where D is a unibranched, one-dimensional, Noetherian, local domain with maximal ideal $\mathfrak{m}$ and finite residue field, as the maximal ideals of the form $\mathfrak{M}_a$ are all distinct in $\operatorname{Int}(D)$ (as recalled above, [6, Remark V.3.2]), it follows that $\mathfrak{q}_\mathfrak{m} = (0)$ and hence, a fortiori, that $\mathfrak{q}_I = (0)$ for every nonzero ideal I of D.

Back to the case of a one-dimensional, Noetherian, local domain D with maximal ideal $\mathfrak{m}$ and finite residue field, unibranched or not unibranched, we want to show there is a power $\mathfrak{m}^k$ of $\mathfrak{m}$ such that the corresponding equalizing ideal is trivial for $\operatorname{Int}(D)$.
By the Krull-Akizuki theorem [17], the integral closure D' of D is a semi-local Dedekind domain. We denote by $\mathfrak{m}'_1, \ldots, \mathfrak{m}'_r$ the maximal ideals of D' and by $\nu_1, \ldots, \nu_r$ the corresponding valuations (thus D is unibranched in case $r = 1$). We can choose $a \in D'$ which is contained in exactly one of the maximal ideals of D', for simplicity we let a be such that $a \in \mathfrak{m}'_1$ and $a \notin \bigcup_{i=2}^r \mathfrak{m}'_i$ (if D is unibranched, we can thus take any non-unit a of D'). The ring $R = D[a]$ is such that $D \subseteq R \subseteq D'$ and is a finitely generated D-module, since a is integral over D. Hence the conductor $(D : R)$ is not trivial and there exists a nonzero element $d \in D$ such that $dR \subseteq D$. With these notations, the following technical lemma exhibits a nonzero ideal I with a trivial equalizing ideal $\mathfrak{q}_I$.

Lemma 3.3.6. *Let D be a one-dimensional, Noetherian, local domain with finite residue field. With the previous notations let $k = \nu_1(d) + 1$ and set $I = {\mathfrak{m}'_1}^k \cap D$. Then $\mathfrak{q}_I = (0)$.*

Proof. The intersection $\eta = \mathfrak{m}'_1 \cap R$ is a maximal ideal of $R = D[a]$. The localization R_η is one-dimensional, Noetherian, obviously local, and its residue field is finite. Moreover, by the choice of a, $\mathfrak{m}'_1$ is the only maximal ideal of D' lying over η and hence, R_η is unibranched (its integral closure is $D'_{\mathfrak{m}'_1}$). As recalled already in several instances, it follows that, for two elements $r \neq s \in R_\eta$ there exists a polynomial $f \in \operatorname{Int}(R_\eta)$ such that $f(r) \in \eta R_\eta$ and $f(s) \notin \eta R_\eta$. The same holds a fortiori for $r, s \in D$. Moreover, as R is Noetherian, we have $\operatorname{Int}(R_\eta) = \operatorname{Int}(R)_\eta$ [6, Theorem I.2.3], and there exists some element $b \in R \setminus \eta$ such that $g = bf \in \operatorname{Int}(R)$. Thus $g(r) \in \eta$ but $g(s) \notin \eta$, that is, $\nu_1(g(r)) \geq 1$ and $\nu_1(g(s)) = 0$. Now, as $d \in (D : R)$, the polynomial $h = dg$ belongs to $\operatorname{Int}(D)$ and $\nu_1(h(r)) = \nu_1(d) + \nu_1(g(r)) \geq k$ while $\nu_1(h(s)) = \nu_1(d) = k - 1$. In other words, $h(r) \in {\mathfrak{m}'_1}^k$ while $h(s) \notin {\mathfrak{m}'_1}^k$. As both $h(r)$ and $h(s)$ are in D and $I = {\mathfrak{m}'_1}^k \cap D$, we thus have $h(r) \in I$ but $h(s) \notin I$, that is, $h \in \mathfrak{I}_{I,r}$ but $h \notin \mathfrak{I}_{I,s}$. Since r and s are arbitrary (but distinct) elements of D we can conclude that $\mathfrak{q}_I = (0)$. □

Still with the same notations, the ideal $I = {\mathfrak{m}'_1}^k \cap D$ clearly contains $\mathfrak{m}^k$. By Proposition 3.3.4 it follows that the equalizing ideal of $\mathfrak{m}^k$ is trivial. Thus we can conclude this section with the following.

Theorem 3.3.7. *Let D be a one-dimensional, local, Noetherian domain with maximal ideal $\mathfrak{m}$ and finite residue field. Then there exists a power $\mathfrak{m}^k$ of $\mathfrak{m}$, such that, for $a \neq b \in D$, $\mathfrak{M}_{k,a} \neq \mathfrak{M}_{k,b}$.*

3.4 Non-finiteness and Skolem closure

The last result of the previous section provides the tools to answer both questions raised in the introduction: for a one-dimensional, Noetherian, local domain D with maximal ideal $\mathfrak{m}$ and finite residue field, 1) the maximal ideals of $\operatorname{Int}(D)$ of the form $\mathfrak{M}_a$ for $a \in D$ are never finitely generated, 2) if D is an almost strong Skolem ring, then D is unibranched.

For the non-finiteness of the ideals $\mathfrak{M}_a$, we could first easily establish (as observed in the introduction) that the ideals $\mathfrak{M}_{k,a}$ for $a \in D$ are not finitely generated. Now each $\mathfrak{M}_{k,a}$ clearly contains the ideal $\mathfrak{m}^k \operatorname{Int}(D)$ of $\operatorname{Int}(D)$ and we prove the following (somewhat stronger) lemma:

Lemma 3.4.1. *Let D be a one-dimensional, Noetherian, local domain with finite residue field. Then, for some power $\mathfrak{m}^k$ of the maximal ideal $\mathfrak{m}$, the ideals $\mathfrak{M}_{k,a}/\mathfrak{m}^k \operatorname{Int}(D)$ of the quotient ring $\operatorname{Int}(D)/\mathfrak{m}^k \operatorname{Int}(D)$ are not finitely generated.*

Proof. From Theorem 3.3.7, there is a power $\mathfrak{m}^k$ of $\mathfrak{m}$ such that $\mathfrak{q}_{\mathfrak{m}^k} = (0)$, that is, the ideals of the form $\mathfrak{M}_{k,a}$ are all distinct. By way of contradiction, suppose that $\mathfrak{M}_{k,a}/\mathfrak{m}^k \operatorname{Int}(D)$ is finitely generated, say by the classes $\overline{f_1}, \dots, \overline{f_n}$ in the quotient ring $\operatorname{Int}(D)/\mathfrak{m}^k \operatorname{Int}(D)$ of polynomials $f_1, \dots, f_n \in \mathfrak{M}_{k,a}$. Now let $g \in \mathfrak{M}_{k,a}$. Then, $g = \sum_{i=1}^n h_i f_i + h$, with each h_i an integer-valued polynomial and $h \in \mathfrak{m}^k \operatorname{Int}(D)$. As $f_i \in \mathfrak{M}_{k,a}$, we have, by definition, $f_i(a) \in \mathfrak{m}^k$. Also, as the polynomials f_i are continuous, there exists a neighborhood U of a such that $f_i(b) \in \mathfrak{m}^k$ for all $b \in U$, that is, $f_i \in \mathfrak{M}_{k,b}$, and thus, a fortiori, $h_i f_i \in \mathfrak{M}_{k,b}$. Finally, as $\mathfrak{M}_{k,b}$ contains $\mathfrak{m}^k \operatorname{Int}(D)$, we have $h \in \mathfrak{M}_{k,b}$. Thus $g \in \mathfrak{M}_{k,b}$. Therefore $\mathfrak{M}_{k,a} \subseteq \mathfrak{M}_{k,b}$, and hence, from Corollary 3.3.3, $\mathfrak{M}_{k,a} = \mathfrak{M}_{k,b}$. We obtain a contradiction for $a \neq b$. □

It follows immediately that $\operatorname{Int}(D)/\mathfrak{m}^k \operatorname{Int}(D)$ is not Noetherian (and a fortiori, neither is $\operatorname{Int}(D)$). This allows to conclude the following theorem.

Theorem 3.4.2. *Let D be a one-dimensional, Noetherian, local domain with finite residue field. Then the maximal ideals $\mathfrak{M}_a$ of $\operatorname{Int}(D)$ are not finitely generated.*

Proof. Lemma 3.4.1 implies that the ideals $\mathfrak{M}_{k,a}/\mathfrak{m}^k \operatorname{Int}(D)$ of $\operatorname{Int}(D)/\mathfrak{m}^k \operatorname{Int}(D)$ are not finitely generated for some power $\mathfrak{m}^k$ of $\mathfrak{m}$, and hence, this quotient ring is not Noetherian. If D is unibranched, we can choose $k = 1$ and the theorem is proved. Thus we can assume that D is not unibranched and hence that all the prime ideals of $\operatorname{Int}(D)$ above $\mathfrak{m}$ are of the form $\mathfrak{M}_a$ for $a \in D$. As a prime containing $\mathfrak{m}^k$ must contain $\mathfrak{m}$, and hence, be above $\mathfrak{m}$, it follows that all the prime ideals of the quotient ring $\operatorname{Int}(D)/\mathfrak{m}^k \operatorname{Int}(D)$ are of the form $\mathfrak{M}_a/\mathfrak{m}^k \operatorname{Int}(D)$. From a theorem by Cohen (see [9]), one of the primes $\mathfrak{M}_a/\mathfrak{m}^k \operatorname{Int}(D)$ of the non-Noetherian ring $\operatorname{Int}(D)/\mathfrak{m}^k \operatorname{Int}(D)$ is not finitely generated. A fortiori, the corresponding maximal ideal $\mathfrak{M}_a$ of $\mathrm{Int}(D)$ is not finitely generated. From the isomorphism $K[X] \xrightarrow{\sim} K[X-a]$, we can conclude that, in fact, none of the maximal ideals $\mathfrak{M}_a$ for $a \in D$ is finitely generated. □

Addressing now the second question, we close this paper with the proof that, under our running hypotheses (of a one-dimensional, Noetherian, local domain D with finite residue field), it is necessary that D is unibranched for $\mathrm{Int}(D)$ to satisfy the almost strong Skolem property.

Theorem 3.4.3. *Let D be a one-dimensional, Noetherian, local domain with maximal ideal $\mathfrak{m}$ and finite residue field $D/\mathfrak{m}$. If D is an almost strong Skolem ring then D is unibranched.*

Proof. By way of contradiction, suppose that D is not unibranched. As already mentioned above (see also [6, Proposition V.3.10]), there are finitely many maximal ideals above $\mathfrak{m}$, all of the form $\mathfrak{M}_a$. Let us denote these ideals by $\mathfrak{M}_1, \dots, \mathfrak{M}_r$. We can choose $f \in \mathfrak{M}_1$ with $f \notin \bigcup_{i=2}^{r} \mathfrak{M}_i$. For $a \in D$, we then have $f(a) \in \mathfrak{m}$ if and only if $\mathfrak{M}_a = \mathfrak{M}_1$. Let $\mathfrak{A} = (\mathfrak{m}, f)$ be the ideal of $\mathrm{Int}(D)$ generated by $\mathfrak{m}$ and f. We then have $\mathfrak{m} \subseteq \mathfrak{A}(a)$ for all $a \in D$. Thus, for $a \in D$, either $\mathfrak{M}_a = \mathfrak{M}_1$, and then $f(a) \in \mathfrak{m}$, and hence, $\mathfrak{A}(a) = \mathfrak{m}$, or $\mathfrak{M}_a \neq \mathfrak{M}_1$, then $f(a) \notin \mathfrak{m}$, and hence $\mathfrak{A}(a) = D$. In other words, $\mathfrak{A}(a) = \mathfrak{M}_1(a)$, for all $a \in D$.
By Theorem 3.4.2 we know that $\mathfrak{M}_1$ is not finitely generated. We can thus choose $g \in \mathfrak{M}_1 \backslash \mathfrak{A}$. Let now $\mathfrak{B} = (\mathfrak{m}, f, g)$. For all $a \in D$, we clearly have $\mathfrak{A}(a) \subseteq \mathfrak{B}(a) \subseteq \mathfrak{M}_1(a)$, and hence, $\mathfrak{A}(a) = \mathfrak{B}(a)$. But $\mathfrak{A} \neq \mathfrak{B}$, whereas both ideals are finitely generated and unitary. We can conclude that, if D is not unibranched, then $\mathrm{Int}(D)$ does not satisfy the almost strong Skolem property. □

Recalling that the condition that D is analytically irreducible is sufficient for $\mathrm{Int}(D)$ to satisfy the almost strong Skolem property ([6, Theorem VII.3.7]), the question to find a condition that is both necessary and sufficient remains open. (Note that, under our hypotheses, D is analytically irreducible if and only if it is unibranched and moreover the integral closure D' of D is finitely generated as a D-module, cf. [6, Proposition III.5.2].)

Example 3.4.4. Let $S = \mathbb{Z}[\sqrt{17}]$. Then S is a non-maximal order in the quadratic number field $K = \mathbb{Q}[\sqrt{17}]$. The maximal order of K is $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{17}}{2}]$; $\mathcal{O}$ is the integral closure of S. It is known, that $\mathcal{O}$ has two different maximal ideals N_1 and N_2 which lie over $2\mathbb{Z}$:

$$N_1 = 2\mathcal{O} + \frac{1+\sqrt{17}}{2}\mathcal{O} \quad \text{and} \quad N_2 = 2\mathcal{O} + \frac{-1+\sqrt{17}}{2}\mathcal{O}$$

Recall that this implies $2\mathcal{O} = N_1 N_2$. It is easily seen that

$$M = 2S + (1+\sqrt{17})S = \{a + b\sqrt{17} \mid a, b \in \mathbb{Z}, a \equiv b \mod 2\}$$

is a maximal ideal of S which lies over $2\mathbb{Z}$. Since $M = N_1 \cap S = N_2 \cap S$, there is no other maximal ideal of S lying over $2\mathbb{Z}$. Let $D = S_M$ be the localization of S at M with maximal ideal $\mathfrak{m} = MD$. Then D is a Noetherian, local and one-dimensional domain with finite residue field. The integral closure D' of D is the localization $(D \setminus M)^{-1}\mathcal{O}$ of $\mathcal{O}$ at M which is not local, since $N_1 D' \neq N_2 D'$ are maximal ideals of D'. In particular, this implies that D is a non-unibranched domain. Let $\eta_i = N_i D'$ $(i = 1, 2)$ denote the maximal ideals of D'. As above, let $\mathfrak{M}_a$ and $\mathfrak{M}_{2,a}$ denote $\mathfrak{I}_{\mathfrak{m},a}$ and $\mathfrak{I}_{\mathfrak{m}^2,a}$, respectively, that is,

$$\mathfrak{M}_a = \{f \in \operatorname{Int}(D) \mid f(a) \in \mathfrak{m}\}$$

and

$$\mathfrak{M}_{2,a} = \{f \in \operatorname{Int}(D) \mid f(a) \in \mathfrak{m}^2\}.$$

We show that

1. $\mathfrak{M}_a = \mathfrak{M}_b$ for all $a, b \in D$ with $a - b \in \mathfrak{m}$.
2. $\mathfrak{M}_{2,a} \neq \mathfrak{M}_{2,b}$ for all $a, b \in D$.

For 1., let $a, b \in D$ with $a - b \in \mathfrak{m}$ and $f \in \operatorname{Int}(D)$ be an integer-valued polynomial on D. Then $f \in K[X]$ is uniformly continuous (on D'_{η_i}) in the $\eta_i D'_{\eta_i}$-adic topology (cf. [6, Proposition III.2.1]), and hence there exists $s_i \geq 1$ such that $x - y \in (\eta_i D'_{\eta_i})^{s_i}$ implies $f(x) - f(y) \in \eta_i D'_{\eta_i}$ for $i = 1, 2$.
By the Chinese Remainder Theorem, there exists $x \in D'$ such that

$$\begin{aligned} x &\equiv a \mod \eta_1^{s_1} \\ x &\equiv b \mod \eta_2^{s_2} \end{aligned}$$

Since $\mathfrak{m}D' \subseteq \eta_i$ and $s_i \geq 1$, it follows that

$$x - b = \underbrace{(x - a)}_{\in \eta_1^{s_1}} + \underbrace{(a - b)}_{\mathfrak{m}} \in \eta_1$$

In particular, this implies that $x - b \in \eta_1 \eta_2 = 2D'$. However, 2 is in the conductor $(S : \mathcal{O})$ which implies that 2 is in the conductor $(D : D')$. Hence $2D' \subseteq D$ which further implies $x \in D$. Therefore $f(a) - f(x) \in \eta_1 D'_{\eta_1} \cap D = \eta_1 D'_{\eta_1} \cap D' \cap D = \eta_1 \cap D = \mathfrak{m}$. Analogously, we deduce $f(b) - f(x) \in \mathfrak{m}$. Therefore

$$f(a) - f(b) = f(a) - f(x) - (f(b) - f(x)) \in \mathfrak{m}$$

Hence $f(a) \equiv f(b) \mod \mathfrak{m}$ for all $f \in \operatorname{Int}(D)$, that is, $\mathfrak{M}_a = \mathfrak{M}_b$.
Next, we show that $\mathfrak{M}_{2,a} \neq \mathfrak{M}_{2,b}$ for all $a, b \in D$. According to Corollary 3.3.3 this is equivalent to $\mathfrak{q}_{\mathfrak{m}^2} = (0)$. Let $I = \eta_1^2 \cap D$. Then $\mathfrak{m}^2 \subseteq I$, and $\mathfrak{q}_I = (0)$ implies $\mathfrak{q}_{\mathfrak{m}^2} = (0)$ according to Proposition 3.3.4.
Let $R = (D')_{\eta_1}$ be the localization of D' at the maximal ideal η_1 with maximal ideal $\eta_1 R$. R is a discrete valuation domain, and by v we denote the discrete valuation of R. Note that

$$\forall\, x \in D : \ (x \in I \iff \mathsf{v}(x) \geq 2)$$

Further, R is analytically irreducible. Therefore, for $a \neq b \in D$, there exists $h \in \mathrm{Int}(R)$ such that $h(a) \in \eta_1 R$ and $h(b) \notin \eta_1 R$. However, by [6, Theorem I.2.3], we know that $h = \frac{g}{s}$ for a $g \in \mathrm{Int}(D')$ and an element $s \in D' \setminus \eta_1$. Hence

$$\mathsf{v}(g(x)) = \mathsf{v}(s) + \mathsf{v}(h(x)) = \mathsf{v}(h(x))$$

for all $x \in D$, since $\mathsf{v}(s) = 0$. Further, we know that $2D' \subseteq D$ and hence $f = 2g \in \mathrm{Int}(D)$. It is easily seen that $\mathsf{v}(2) = 1$ and therefore

$$\mathsf{v}(f(x)) = \mathsf{v}(2) + \mathsf{v}(g(x)) = 1 + \mathsf{v}(h(x))$$

for all $x \in D$. In particular, we know that $\mathsf{v}(f(a)) \geq 2$ (since $\mathsf{v}(h(a)) \geq 1$) and $\mathsf{v}(f(b)) = 1$. Therefore $f(a) \in I$ and $f(b) \notin I$ which implies $\mathfrak{q}_I = (0)$.

Bibliography

[1] N. Bourbaki. *Commutative Algebra, Chapters 1-7*. Springer, Berlin, 1989.

[2] W. C. Brown. *Matrices over Commutative Rings*. Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, Inc., New York, 1993.

[3] W. C. Brown. *Null ideals and spanning ranks of matrices*. *Comm. Algebra* 26.8 (1998), pp. 2401–2417. ISSN: 0092-7872. DOI: 10.1080/00927879808826285.

[4] W. C. Brown. *Null ideals and spanning ranks of matrices. II*. *Comm. Algebra* 27.12 (1999), pp. 6051–6067. ISSN: 0092-7872. DOI: 10.1080/00927879908826807.

[5] W. C. Brown. *Null Ideal of Matrices*. *Communications in Algebra* 33 (2005), pp. 4491–4504.

[6] P.-J. Cahen and J.-L. Chabert. *Integer-Valued Polynomials*. American Mathematical Society, 1997.

[7] P.-J. Cahen and J.-L. Chabert. *Skolem properties and integer-valued polynomials: a survey*. *Advances in commutative ring theory (Fez, 1997)*. Vol. 205. Lecture Notes in Pure and Appl. Math. New York: Dekker, 1999, pp. 175–195.

[8] P.-J. Cahen and R. Rissner. *Finiteness and Skolem closure of ideals for nonunibranched domains*. *Communications in Algebra* 43 (2015), pp. 2231–2239. DOI: 10.1080/00927872.2013.879159.

[9] I. S. Cohen. *Commutative rings with restricted minimum condition*. *Duke Mathematical Journal* 17 (1950), pp. 27–42.

[10] S. Evrard, Y. Fares, and K. Johnson. *Integer valued polynomials on lower triangular integer matrices*. *Monatsh. Math.* 170 (2013), pp. 147–160. ISSN: 0026-9255. DOI: 10.1007/s00605-013-0481-6.

[11] S. Frisch. *Integrally closed domains, minimal polynomials, and null ideals of matrices*. *Communications in Algebra* 32(5) (2004), pp. 2015–2017.

[12] S. Frisch. *Integer-valued polynomials on algebras - a survey*. *Actes du CIRM* 2 (2010), pp. 27–32.

[13] S. Frisch. *Integer-valued polynomials on algebras*. *J. Algebra* 373 (2013), pp. 414–425. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2012.10.003.

[14] H. Gunji and D. L. McQuillan. *On rings with a certain divisibility property*. *Michigan Math. Journal* 22 (1976), pp. 289–299.

[15] S. Lang. *Algebra*. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag New York, 2002.

[16] K. A. Loper and N. J. Werner. *Generalized rings of integer-valued polynomials. J. Number Theory* 132.11 (2012), pp. 2481–2490. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2012.05.009.

[17] H. Matsumura. *Commutative Algebra.* Cambridge University Press, 1986.

[18] M. Nagata. *Local rings.* Vol. 13. Interscience Tracts in Pure and Applied Mathematics. Interscience Publishers a division of John Wiley & Sons, 1962.

[19] G. Peruginelli. *Integer-valued polynomials over matrices and divided differences. Monatsh. Math.* 173.4 (2014), pp. 559–571. ISSN: 0026-9255. DOI: 10.1007/s00605-013-0519-9.

[20] G. Peruginelli and N. Werner. *Integral closure of rings of integer-valued polynomials on algebras. Commutative Algebra: Recent Advances in Commutative Rings, Integer-Valued Polynomials, and Polynomial Functions.* Editors: Fontana, M. and Frisch, S. and Glaz, S. Springer, 2014.

[21] D. Rees. *Lectures on the Asymptotic Theory of Ideals.* London Mathematical Society Lecture Note Series 113. Cambridge University Press, 1988.

[22] R. Rissner. *Null ideal of matrices over residue class rings of principal ideal domains. Submitted* (2015).

[23] S. Roman. *Advanced Linear Algebra.* 3rd. Vol. 135. Graduate Texts in Mathematics. Springer-Verlag, New York, 2008.

[24] T. Skolem. *Ein Satz über ganzwertige Polynome. Det Kongelige Norske Videnskabers Selskab (Trondheim)* 9 (1936), pp. 111–113.