Journal of Algebra 460 (2016) 320–339

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Properly integral polynomials over the ring of integer-valued polynomials on a matrix ring

Giulio Peruginelli [a], Nicholas J. Werner [b,*]

[a] Department of Mathematics, University of Padova, Via Trieste, 63 35121 Padova, Italy

[b] Department of Mathematics, Computer and Information Science, SUNY College at Old Westbury, Old Westbury, NY 11568, United States

A R T I C L E I N F O

Article history:
Received 29 June 2015
Available online xxxx
Communicated by Luchezar L. Avramov

MSC:
primary 13F20
secondary 13B22, 11C99

Keywords:
Integer-valued polynomial
Integral closure
Null ideal
Matrix ring
P-sequence

A B S T R A C T

Let D be a domain with fraction field K, and let $M_n(D)$ be the ring of $n \times n$ matrices with entries in D. The ring of integer-valued polynomials on the matrix ring $M_n(D)$, denoted $\mathrm{Int}_K(M_n(D))$, consists of those polynomials in $K[x]$ that map matrices in $M_n(D)$ back to $M_n(D)$ under evaluation. It has been known for some time that $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ is not integrally closed. However, it was only recently that an example of a polynomial in the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ but not in the ring itself appeared in the literature, and the published example is specific to the case $n = 2$. In this paper, we give a construction that produces polynomials that are integral over $\mathrm{Int}_K(M_n(D))$ but are not in the ring itself, where D is a Dedekind domain with finite residue fields and $n \geq 2$ is arbitrary. We also show how our general example is related to P-sequences for $\mathrm{Int}_K(M_n(D))$ and its integral closure in the case where D is a discrete valuation ring.

* Corresponding author.
E-mail addresses: gperugin@math.unipd.it (G. Peruginelli), wernern@oldwestbury.edu (N.J. Werner).

http://dx.doi.org/10.1016/j.jalgebra.2016.04.016

1. Introduction

When D is a domain with field of fractions K, the ring of integer-valued polynomials on D is $\text{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\}$. Such rings have been extensively studied over the past several decades; the reader is referred to [5] for standard results on these objects. More recently, attention has turned to the consideration of integer-valued polynomials on algebras [6,8–12,17,18,20–23]. The typical approach for this construction is to take a torsion-free D-algebra A that is finitely generated as a D-module and such that $A \cap K = D$. Then, we define $\text{Int}_K(A)$ to be the set of polynomials in $K[x]$ that map elements of A back to A under evaluation. That is, $\text{Int}_K(A) := \{f \in K[x] \mid f(A) \subseteq A\}$, which is a subring of $\text{Int}(D)$. (Technically, evaluation of $f \in K[x]$ at elements of A is performed in the tensor product $K \otimes_D A$ by associating K and A with their canonical images $K \otimes 1$ and $1 \otimes A$. In practice, however, it is usually clear how to perform the evaluation without the formality of tensor products.)

Depending on the choice of A, the ring $\text{Int}_K(A)$ can exhibit similarities to, or stark differences from, $\text{Int}(D)$. For instance, if A is the ring of integers of a number field (viewed as a $\mathbb{Z}$-algebra), then $\text{Int}_{\mathbb{Q}}(A)$ is—like $\text{Int}(\mathbb{Z})$—a Prüfer domain [17, Thm. 3.7], hence is integrally closed. In contrast, when $A = M_n(\mathbb{Z})$ is the algebra of $n \times n$ matrices with entries in $\mathbb{Z}$, $\text{Int}_{\mathbb{Q}}(A)$ is not integrally closed (although its integral closure is a Prüfer domain) [17, Sec. 4]. In a more general setting, it is known [5, Thm. VI.1.7] that if D is a Dedekind domain with finite residue fields, then $\text{Int}(D)$ is a Prüfer domain, and so is integrally closed. The motivation for this paper was to show, by giving a form for a general counterexample, that $\text{Int}_K(M_n(D))$ is not integrally closed. In this vein, we make the following definition.

Definition 1.1. A polynomial $f \in K[x]$ will be called *properly integral* over $\text{Int}_K(A)$ if f lies in the integral closure of $\text{Int}_K(A)$, but $f \notin \text{Int}_K(A)$.

Note that the integral closure of $\text{Int}_K(A)$ in its field of fractions $K(x)$ is contained in $K[x]$, so that $\text{Int}_K(A)$ is integrally closed if and only if there are no properly integral polynomials over $\text{Int}_K(A)$. It has been known for some time that $\text{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ is not integrally closed. However, the first published example of a properly integral polynomial over $\text{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ was given only recently by Evrard and Johnson in [9], and only for the case $n = 2$. We will give a general construction for a properly integral polynomial over $\text{Int}_K(M_n(D))$, where D is a Dedekind domain with finite residue rings, and $n \geq 2$ is arbitrary.

The theorems in this paper can be seen as complementary to the work of Evrard and Johnson. Their results relied heavily on the P-orderings and P-sequences of Bhargava [4] and the generalizations of these in [15]. In the case where $D = \mathbb{Z}$, a properly integral polynomial $f(x) = g(x)/p^k$ (where $g \in \mathbb{Z}[x]$, p^k is a prime power, and p does not divide g) over $\text{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ produced by using the methods and p-sequences in [9] is optimal in the sense that f has minimal degree among all properly integral polynomials of the form

$g_1(x)/p^{k_1}$, where $k_1 > 0$. However, building such an f requires knowing the p-sequences for $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ and its integral closure. In general, these sequences are quite difficult to determine; to date, formulas for such p-sequences have been given only in the case $n = 2$. In contrast, our construction gives a properly integral polynomial for a much larger variety of rings and does not require a P-sequence, but it is only known to be optimal when $n = 2$ and $D = \mathbb{Z}$—a fact we can prove precisely because of the p-sequences derived in [9].

The paper proceeds as follows. Section 2 begins with a concrete construction for a properly integral polynomial over $\mathrm{Int}_K(M_n(D))$ that works when D is a discrete valuation ring (DVR). This local result is then globalized (Theorem 3.3) in Section 3 to the case where D is a Dedekind domain. We also point out (Corollary 3.5) that the same construction works for some algebras that are not matrix rings. Section 4 relates our work to the P-sequences used by Evrard and Johnson. We generalize (Theorem 4.10) a classical theorem known to Dickson [7, Thm. 27, p. 22] concerning the ideal of polynomials in $\mathbb{Z}[x]$ whose values over $\mathbb{Z}$ are divisible by a fixed prime power p^k, $k \leq p$, and use this generalization to give a concise formula (Corollary 4.20) for the initial terms of the P-sequence for $\mathrm{Int}_K(M_n(V))$, where V is a DVR and $n \geq 2$. Finally, by utilizing the formulas given in [9] for the p-sequences of the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}))$, we prove that the polynomials produced by our construction are optimal (in the sense of the previous paragraph) when $D = \mathbb{Z}$ and $n = 2$ (Corollary 4.21).

2. Construction of the properly integral polynomial

Let V be a discrete valuation ring (DVR) with maximal ideal πV, field of fractions K, and finite residue field $V/\pi V \cong \mathbb{F}_q$. Fix an algebraic closure $\overline{K}$ of K and for each $n \geq 2$, let $\Lambda_n(V)$ be the set of elements of $\overline{K}$ whose degree over V is at most n. For each $\alpha \in \Lambda_n(V)$, we let O_α be the integral closure of V in $K(\alpha)$.

We know [22, Cor. 16] that the integral closure of $\mathrm{Int}_K(M_n(V))$ is equal to

$$\mathrm{Int}_K(\Lambda_n(V)) := \{f \in K[x] \mid f(\Lambda_n(V)) \subseteq \Lambda_n(V)\}.$$

Note that since $\Lambda_n(V) \cap K(\alpha) = O_\alpha$, we have $f \in \mathrm{Int}_K(\Lambda_n(V))$ if and only if $f(\alpha) \in O_\alpha$ for each $\alpha \in \Lambda_n(V)$. Here, we will give a general construction for a polynomial F that is properly integral over $\mathrm{Int}_K(M_n(V))$; that is, $F \in \mathrm{Int}_K(\Lambda_n(V)) \setminus \mathrm{Int}_K(M_n(V))$. The idea behind the construction is as follows.

A polynomial $f \in K[x]$ is integer-valued on $M_n(V)$ if and only if it is integer-valued on the set of $n \times n$ companion matrices in $M_n(V)$ [10, Thm. 6.3]. It turns out that if f is integer-valued on "enough" companion matrices, then it can still lie in $\mathrm{Int}_K(\Lambda_n(V))$. However, as long as f is not integer-valued on at least one companion matrix, f will not be in $\mathrm{Int}_K(M_n(V))$. So, we will build a polynomial that is integer-valued on almost all of the companion matrices in $M_n(V)$; specifically, our polynomial will fail to be integer-valued on the set of companion matrices whose characteristic polynomial mod π is a power of a linear polynomial.

As part of our construction, we will lift elements from $\mathbb{F}_q$ or $\mathbb{F}_q[x]$ up to V or $V[x]$. To be precise, one should first pick residue representatives for $\mathbb{F}_q$ and $\mathbb{F}_q[x]$, and then use these in all calculations taking place over V. However, to ease the notation, we will write $\mathbb{F}_q$ throughout. When a calculation must be performed over the finite field, we will say it occurs "mod π" or "in $\mathbb{F}_q$".

Construction 2.1. Let $n \geq 2$. Let

$$\begin{aligned}
\mathscr{P} &= \{f \in \mathbb{F}_q[x] \mid f \text{ is monic, irreducible, and } 2 \leq \deg f \leq n\},\\
\theta(x) &= \prod_{f \in \mathscr{P}} f(x)^{\lfloor n/\deg f \rfloor},\\
h(x) &= x^{n-1} \prod_{a \in \mathbb{F}_q^\times} (x^n + \pi a),\\
H(x) &= \prod_{b \in \mathbb{F}_q} h(x-b), \text{ and finally}\\
F(x) &= \frac{H(x)(\theta(x))^q}{\pi^q}.
\end{aligned}$$

The simplest example for F occurs when $n = 2$ and $V = \mathbb{Z}_{(2)}$, so that $q = 2$. Then, we have

$$F(x) = \frac{x(x^2+2)(x-1)((x-1)^2+2)(x^2+x+1)^2}{4}.$$

Our main result is the following.

Theorem 2.2. *Let F be as in Construction 2.1. Then, F is properly integral over $\mathrm{Int}_K(M_n(V))$.*

Remark 2.3. Even if one specifies a degree d_0 and a denominator d, properly integral polynomials of the form $g(x)/d$ with $\deg g = d_0$ are not unique. Indeed, [9, Cor. 3.6] shows that

$$G(x) = \frac{x(x^2+2x+2)(x-1)(x^2+1)(x^2-x+1)(x^2+x+1)}{4}$$

is properly integral over $\mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}_{(2)}))$, and clearly G is not equal to the F given above. However, one may prove the following. Let I be the ideal of $\mathbb{Z}_{(2)}[x]$ generated by 4 and $2x^2(x-1)^2(x^2+x+1)$. If $G_1, G_2 \in \mathbb{Z}_{(2)}[x]$ are both monic of degree 10 and both $F_1 = G_1/4$ and $F_2 = G_2/4$ are properly integral over $\mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}_{(2)}))$, then G_1 and G_2 are equivalent modulo I. As one may check, this is the case with F and G. Similar equivalences are possible for other choices of V, d_0, and d.

One part of Theorem 2.2 is easy to prove. The remaining parts are more involved, and the proof is completed at the end of Section 2.

Lemma 2.4. *$F \notin \mathrm{Int}_K(M_n(V))$.*

Proof. Let $C \in M_n(V)$ be the companion matrix for x^n. Then, $(\prod_{a\in\mathbb{F}_q^\times} h(C-aI))(\theta(C))^q$ is a unit mod π, hence is also a unit mod π^q. So, the only way that $F(C)$ will be in $M_n(V)$ is if $h(C)$ is 0 mod π^q. However,

$$h(C) = C^{n-1}\prod_{a\in\mathbb{F}_q^\times}(C^n + \pi a I) = C^{n-1}\prod_{a\in\mathbb{F}_q^\times}(\pi a)I$$

is only divisible by $q-1$ powers of π. Thus, $h(C) \notin \pi^q M_n(V)$, $F(C) \notin M_n(V)$, and $F \notin \mathrm{Int}_K(M_n(V))$. Note that the same steps work if we replace x^n by $(x-a)^n$, where $a \in \mathbb{F}_q^\times$, and replace $h(x)$ with $h(x-a)$. $\square$

Remark 2.5. The failure of F to lie in $\mathrm{Int}_K(M_n(V))$ can also be expressed in terms of pullback rings. By [18, Rem. 2.1 & (3)]), we have

$$\mathrm{Int}_K(M_n(V)) = \bigcap_{f\in\mathcal{P}_n}(V[x] + f(x)K[x]),$$

where $\mathcal{P}_n$ is the set of monic polynomials in $V[x]$ of degree exactly equal to n. The previous Claim then demonstrates that $F \notin V[x] + (x-a)^n K[x]$ for any $a \in \mathbb{F}_q$.

Showing that $F \in \mathrm{Int}_K(\Lambda_n(V))$ is more difficult. The general idea is to take $\alpha \in \Lambda_n(V)$ and focus on its minimal polynomial $m(x)$ over V. We then consider two possibilities, according to how the polynomial $m(x)$ factors over the residue field. Either $m(x) \equiv (x-a)^n \bmod \pi$, for some $a \in \mathbb{F}_q$; or $m(x) \not\equiv (x-a)^n \bmod \pi$, for all $a \in \mathbb{F}_q$. The first case is the more difficult one, and occupies the next several results. The second case is dealt with in Lemma 2.10, right before we complete the proof of Theorem 2.2.

So, for now we concentrate on those cases where $m(x) \equiv (x-a)^n \bmod \pi$ for some $a \in \mathbb{F}_q$. In fact, by translation, it will be enough to consider the case where $m(x) \equiv x^n \bmod \pi$. Our starting point is a lemma involving symmetric polynomials. Given a set $S = \{x_1, x_2, \ldots, x_n\}$, for each $1 \le k \le n$, we let $\sigma_k(S)$ denote the kth elementary symmetric polynomial in $x_1, x_2, \ldots, x_n$.

Lemma 2.6. *Let $\overline{V}$ be the integral closure of V in $\overline{K}$. Let $n \ge 2$, let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset \overline{V}$, and let $S^{n-1} = \{\alpha_1^{n-1}, \alpha_2^{n-1}, \ldots, \alpha_n^{n-1}\}$. Assume the following:*

- *$\sigma_k(S) \in \pi V$, for all $1 \le k \le n-1$.*
- *$\sigma_n(S) \in \pi^2 V$.*

Then, $\sigma_k(S^{n-1}) \in \pi^k V$ for each $1 \le k \le n$.

Proof. The stated conditions ensure that $\prod_{k=1}^{n}(x-\alpha_k) \in V[x]$. In particular, $S \subset \Lambda_n(V)$ and the set of conjugates of each α_k is contained in S. From this, it follows that the polynomial $\prod_{k=1}^{n}(x - \alpha_k^{n-1})$ is also in $V[x]$, and thus that $\sigma_k(S^{n-1}) \in V$ for each k. It remains to show that π^k divides $\sigma_k(S^{n-1})$.

Fix k between 1 and n and consider $\sigma_k(S^{n-1})$. By "total degree" we mean degree as a polynomial in $\alpha_1, \alpha_2, \dots, \alpha_n$. Thus, each element of S^{n-1} has total degree $n-1$; each monomial of $\sigma_k(S^{n-1})$ has total degree $k(n-1)$; and $\sigma_k(S^{n-1})$, being homogeneous in $\alpha_1, \alpha_2, \dots, \alpha_n$, also has total degree $k(n-1)$. By the Fundamental Theorem of Symmetric Polynomials, $\sigma_k(S^{n-1})$ equals a polynomial f in $\sigma_1(S), \sigma_2(S), \dots, \sigma_n(S)$. Moreover, each monomial $a\sigma_1(S)^{e_1}\sigma_2(S)^{e_2}\cdots\sigma_n(S)^{e_n}$ in f has total degree (as a polynomial in $\alpha_1, \alpha_2, \dots, \alpha_n$) equal to $k(n-1)$. It suffices to prove that each such monomial in f is divisible by π^k.

Let v denote the natural valuation for V and let $\beta = a\sigma_1(S)^{e_1}\sigma_2(S)^{e_2}\cdots\sigma_n(S)^{e_n}$ be a monomial of f in $\sigma_1(S), \sigma_2(S), \dots, \sigma_n(S)$. Since the total degree of β is $k(n-1)$, we obtain

$$e_1 + 2e_2 + \cdots + ne_n = k(n-1). \tag{2.7}$$

Also, by assumption,

$$\begin{aligned} v(\beta) &\geq v(\sigma_1(S)^{e_1}) + v(\sigma_2(S)^{e_2}) + \cdots + v(\sigma_n(S)^{e_n}) \\ &\geq e_1 + e_2 + \cdots + e_{n-1} + 2e_n. \end{aligned}$$

We want to show that $v(\beta) \geq k$. From (2.7), we have

$$\begin{aligned} k &= \frac{e_1}{n-1} + \frac{2e_2}{n-1} + \cdots + \frac{(n-1)e_{n-1}}{n-1} + \frac{ne_n}{n-1} \\ &\leq e_1 + e_2 + \cdots + e_{n-1} + 2e_n \\ &\leq v(\beta), \end{aligned}$$

as desired. □

Lemma 2.6 is used to prove the first part of the next proposition.

Proposition 2.8. *Let $\alpha \in \Lambda_n(V)$ with minimal polynomial over V equal to $m(x) = x^n + \pi a_{n-1}x^{n-1} + \cdots + \pi a_1 x + \pi a_0$, where each $a_k \in V$.*

(1) *If $a_0 \in \pi V$, then $\alpha^{n-1}/\pi \in O_\alpha$.*
(2) *If $a_0 \notin \pi V$, then $(\alpha^{n-1}(\alpha^n + \pi a))/\pi^2 \in O_\alpha$, where $a \in \mathbb{F}_q$ is the residue of a_0 mod π.*

Proof. (1) Assume $a_0 \in \pi V$. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of m. Let $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ and $S^{n-1} = \{\alpha_1^{n-1}, \alpha_2^{n-1}, \dots, \alpha_n^{n-1}\}$. Then, the conditions of Lemma 2.6

are satisfied, so $\sigma_k(S^{n-1}) \in \pi^k V$ for each $1 \le k \le n$. Let $g(x) = \prod_{k=1}^n (x - \alpha_k^{n-1}/\pi)$. Then, the coefficient of x^{n-k} in $g(x)$ is $(-1)^{n-k}\sigma_k(S^{n-1})/\pi^k \in V$. Thus, $g \in V[x]$ and $g(\alpha^{n-1}/\pi) = 0$, so $\alpha^{n-1}/\pi \in O_\alpha$.

(2) Assume $a_0 \notin \pi V$. Let $a' \in V$ be such that $a - a_0 = \pi a'$. Since $m(\alpha) = 0$, we have

$$\alpha^n = -\pi a_{n-1}\alpha^{n-1} - \cdots - \pi a_1 \alpha - \pi a_0.$$

In particular, this means that $\alpha^n \in \pi O_\alpha$. Next,

$$\begin{aligned}\alpha^{n-1}(\alpha^n + \pi a) &= \alpha^{n-1}(-\pi a_{n-1}\alpha^{n-1} - \cdots - \pi a_1\alpha - \pi a_0 + \pi a) \\ &= \alpha^{n-1}(-\pi a_{n-1}\alpha^{n-1} - \cdots - \pi a_1 \alpha + \pi^2 a').\end{aligned}$$

For each $1 \le k \le n-1$, $\alpha^{n-1}(\pi a_k \alpha^k)$ is divisible by both π and α^n, so $\alpha^{n-1}(\pi a_k\alpha^k) \in \pi^2 O_\alpha$. Also, $\alpha^{n-1}\pi^2 a' \in \pi^2 O_\alpha$. It now follows that $(\alpha^{n-1}(\alpha^n + \pi a))/\pi^2 \in O_\alpha$. □

Now, we relate Proposition 2.8 to the polynomial from Construction 2.1.

Proposition 2.9. *Let $\alpha \in \Lambda_n(V)$ have minimal polynomial $m(x)$ such that $m(x) \equiv x^n \bmod \pi$. Let $f(x) = h(x)/\pi^q$, where h is as in Construction 2.1. Then, $f(\alpha) \in O_\alpha$.*

Proof. Since $m(x) \equiv x^n \bmod \pi$, we have $m(x) = x^n + \pi a_{n-1}x^{n-1} + \cdots + \pi a_1 x + \pi a_0$ for some $a_0, \ldots, a_{n-1} \in V$. Note that for $a \in \mathbb{F}_q^\times$, we have $(\alpha^n + \pi a)/\pi \in O_\alpha$.

If $a_0 \in \pi V$, then $\alpha^{n-1}/\pi \in O_\alpha$ by Proposition 2.8 part (1). In this case,

$$f(\alpha) = \frac{\alpha^{n-1}}{\pi} \prod_{a \in \mathbb{F}_q^\times} \frac{\alpha^n + \pi a}{\pi}$$

is an element of O_α.

If $a_0 \notin \pi V$, then by Proposition 2.8 part (2), there exists $a \in \mathbb{F}_q^\times$ such that $(\alpha^{n-1}(\alpha^n + \pi a))/\pi^2 \in O_\alpha$. This time, we group the factors of $f(\alpha)$ as

$$f(\alpha) = \frac{\alpha^{n-1}(\alpha^n + \pi a)}{\pi^2} \prod_{\substack{b \in \mathbb{F}_q^\times, \\ b \neq a}} \frac{\alpha^n + \pi b}{\pi}$$

and as before we see that $f(\alpha) \in O_\alpha$. □

Proposition 2.9 is what we ultimately need to prove Theorem 2.2. As mentioned after Remark 2.5, there is a second case to consider, in which an element $\alpha \in \Lambda_n(V)$ has a minimal polynomial $m(x)$ such that $m(x) \not\equiv (x-a)^n \bmod \pi$, for all $a \in \mathbb{F}_q$. Most of the work required in this case is done in the next lemma.

Lemma 2.10. *Let $\alpha \in \Lambda_n(V)$ with minimal polynomial $m(x)$ such that $m(x) \not\equiv (x-a)^n$ mod π, for all $a \in \mathbb{F}_q$. Then the numerator of F admits a factorization $H(x)(\theta(x))^q = \prod_{b\in\mathbb{F}_q} f_b(x)$ such that $m(x)$ divides $f_b(x)$ mod π for each b. Consequently, $F(\alpha) \in O_\alpha$.*

Proof. We have

$$\begin{aligned} H(x) &= \prod_{b\in\mathbb{F}_q} h(x-b) \\ &= \prod_{b\in\mathbb{F}_q} \Big[(x-b)^{n-1} \prod_{a\in\mathbb{F}_q^\times} ((x-b)^n + \pi a)\Big] \\ &= \Big[\prod_{b\in\mathbb{F}_q} (x-b)^{n-1}\Big]\Big[\prod_{a\in\mathbb{F}_q^\times} \prod_{b\in\mathbb{F}_q} ((x-b)^n + \pi a)\Big]. \end{aligned}$$

Let $f_0(x) = (\prod_{b\in\mathbb{F}_q}(x-b)^{n-1})\theta(x)$ and for each $a \in \mathbb{F}_q^\times$, let $f_a(x) = (\prod_{b\in\mathbb{F}_q}((x-b)^n + \pi a))\theta(x)$. Then, $H(x)(\theta(x))^q = \prod_{b\in\mathbb{F}_q} f_b(x)$.

Now, factor $m(x)$ mod π as

$$m(x) \equiv \iota_1(x)^{n_1}\iota_2(x)^{n_2}\cdots\iota_t(x)^{n_t}$$

where each ι_k is a distinct monic irreducible polynomial in $\mathbb{F}_q[x]$. Assuming that $m(x) \not\equiv (x-a)^n$ mod π for any $a \in \mathbb{F}_q$, each exponent n_k satisfies $1 \le n_k \le \lfloor n/\deg(\iota_k)\rfloor < n$ if $\deg(\iota_k) > 1$ or $1 \le n_k < n$ if $\deg(\iota_k) = 1$. So, working mod π, the product of the $\iota_k^{n_k}$ with $\deg(\iota_k) > 1$ divides θ; and the product of the $\iota_k^{n_k}$ with $\deg(\iota_k) = 1$ divides f_b/θ for each $b \in \mathbb{F}_q$. Hence, $m(x)$ divides $f_b(x)$ mod π. Finally, the last condition implies that $f_b(\alpha) \in \pi O_\alpha$ for each b. Thus, $H(\alpha)(\theta(\alpha))^q = \prod_{b\in\mathbb{F}_q} f_b(\alpha) \in \pi^q O_\alpha$, and so $F(\alpha) \in O_\alpha$. $\square$

Finally, we complete the proof of Theorem 2.2. For convenience, the theorem is restated below.

Theorem 2.2. *Let the notation be as in Construction 2.1. Then, F is properly integral over $\mathrm{Int}_K(M_n(V))$.*

Proof. The polynomial $F \notin \mathrm{Int}_K(M_n(V))$ by Lemma 2.4. To show that $F \in \mathrm{Int}_K(\Lambda_n(V))$, let $\alpha \in \Lambda_n(V)$. We will prove that $F(\alpha) \in O_\alpha$.

Let $m(x)$ be the minimal polynomial of α. If $m(x) \equiv (x-a)^n$ mod π for some $a \in \mathbb{F}_q$, then by Proposition 2.9 we have $h(\alpha - a)/\pi^q \in O_\alpha$. Hence, $F(\alpha) \in O_\alpha$ in this case. If instead $m(x) \not\equiv (x-a)^n$ mod π for all $a \in \mathbb{F}_q$, then by Lemma 2.10 we still have $F(\alpha) \in O_\alpha$. $\square$

3. Globalization and extension to algebras

In this section, we discuss how to globalize Construction 2.1, and demonstrate that it is applicable to algebras other than matrix rings.

Thus far, we have focused on the local case and worked with the DVR V. However, since the formation of our integer-valued polynomial rings is well-behaved with respect to localization, our results can be applied to the global case where V is replaced with a Dedekind domain. For the remainder of this section, D will denote a Dedekind domain with finite residue fields. As with V, we let K be the fraction field of D and we fix an algebraic closure $\overline{K}$ of K. For $n \geq 2$, let $\Lambda_n(D)$ be the set of elements of $\overline{K}$ whose degree over D is at most n. Then, by [22, Cor. 16], the integral closure of $\mathrm{Int}_K(M_n(D))$ is $\mathrm{Int}_K(\Lambda_n(D))$. By taking $V = D_P$ for a nonzero prime P of D, we can use our local construction to produce polynomials that are properly integral over $\mathrm{Int}_K(M_n(D))$. Most of the work is done in the following lemma, which works over any integral domain D.

Lemma 3.1. *Let R and S be D-modules such that $D[x] \subseteq R \subseteq S \subseteq K[x]$. Assume there exists a nonzero prime P of D such that $R_P \subsetneq S_P$, and let $f \in S_P \setminus R_P$. Then, there exists $c \in D \setminus P$ such that $cf \in S \setminus R$.*

Proof. Write $f(x) = g(x)/d$, where $g \in S$, $d \in D \setminus P$, and d does not divide g. Since $f(x)$ is not in R_P, $g \notin R$. Hence, $df = g \in S \setminus R$, as wanted. $\square$

We also require a result regarding the localization of $\mathrm{Int}_K(A)$ at primes of D.

Proposition 3.2. *([23, Prop. 3.1, 3.2]) Let A be a torsion-free D-algebra that is finitely generated as D-module and such that $A \cap K = D$. Then, $\mathrm{Int}_K(A)_Q = \mathrm{Int}_K(A_Q)$ for each nonzero prime Q of D, and $\mathrm{Int}_K(A) = \bigcap_Q \mathrm{Int}_K(A)_Q$, where the intersection is over all nonzero primes Q of D.*

Combining Construction 2.1 with Lemma 3.1 now allows us to produce polynomials that are properly integral over $\mathrm{Int}_K(M_n(D))$.

Theorem 3.3. *Let P be a nonzero prime of D. Let $V = D_P$ and let F be the polynomial from Construction 2.1 applied to V. Then, there exists $c \in D \setminus P$ such that cF is properly integral over $\mathrm{Int}_K(M_n(D))$. In particular, if P is principal, then we can take $c = 1$.*

Proof. By Proposition 3.2, $\mathrm{Int}_K(M_n(D))_P = \mathrm{Int}_K(M_n(V))$, and a similar argument shows that $\mathrm{Int}_K(\Lambda_n(D))_P = \mathrm{Int}_K(\Lambda_n(V))$. So, we can apply Lemma 3.1 with $R = \mathrm{Int}_K(M_n(D))$, $S = \mathrm{Int}_K(\Lambda_n(D))$, and $f = F$. Furthermore, if P is principal, then we can assume the denominator π^q of F is in D and that $P = \pi D$. In this case, it is immediately seen that F itself is already an element of $S \setminus R$, since $F \in S_Q$ for every prime ideal Q of D different from P and $S = \bigcap_Q S_Q$, the intersection ranging over the set of all non-zero prime ideals of D. $\square$

Corollary 3.4. *Let D be a Dedekind domain with finite residue fields. Let K be the field of fractions of D and let $n \geq 2$. Then,* $\mathrm{Int}_K(M_n(D))$ *is not integrally closed.*

Finally, we show that the polynomial in Construction 2.1 can be applied to D-algebras other than matrix rings. Consider a torsion-free D-algebra A that is finitely generated as a D-module and such that $A \cap K = D$. If A has a generating set consisting of at most n elements, then each element of A satisfies a monic polynomial in $D[x]$ of degree at most n (see for example [2, Thm. 1, Chap. V] or [1, Prop. 2.4, Chap. 2]). It is then a consequence of [13, Lem. 3.4] that $\mathrm{Int}_K(M_n(D)) \subseteq \mathrm{Int}_K(A)$, and thus that the integral closure of $\mathrm{Int}_K(A)$ contains $\mathrm{Int}_K(\Lambda_n(D))$.

Corollary 3.5. *Let D and A be as above. Assume that there exists a nonzero prime P of D such that $A/P^qA \cong M_n(D/P^q)$, where $q = |D/P|$. Let cF be as in Theorem 3.3. Then, cF is properly integral over* $\mathrm{Int}_K(A)$*. Thus,* $\mathrm{Int}_K(A)$ *is not integrally closed.*

Proof. The polynomial cF is in the integral closure of $\mathrm{Int}_K(A)$ because this integral closure contains $\mathrm{Int}_K(\Lambda_n(D))$. To show that $cF \notin \mathrm{Int}_K(A)$, we will work with localizations. Localize the algebra A in the natural way to produce the D_P-algebra A_P. Let π be the generator of PD_P. Then, for all $k > 0$, we have $A_P/\pi^k A_P = A_P/P^k A_P \cong A/P^k A$. In particular, $A_P/\pi^q A_P \cong M_n(D/P^q)$.

Now, by Proposition 3.2, we see that $\mathrm{Int}_K(A)_Q = \mathrm{Int}_K(A_Q)$ for all nonzero primes Q of D, and $\mathrm{Int}_K(A) = \bigcap_Q \mathrm{Int}_K(A)_Q$. So, to prove that $cF \notin \mathrm{Int}_K(A)$, it suffices to show that $cF \notin \mathrm{Int}_K(A_P)$, and since c is a unit of D_P, it will be enough to demonstrate that $F \notin \mathrm{Int}_K(A_P)$. Suppose by way of contradiction that $F \in \mathrm{Int}_K(A_P)$. Then, the numerator G of F is such that $G(A_P) \subseteq \pi^q A_P$; equivalently, $G(A_P/\pi^q A_P)$ is 0 mod π^q. However, because $A_P/\pi^q A_P \cong M_n(D/P^q)$, the argument used Lemma 2.4 shows that this is impossible. Thus, we conclude that $F \notin \mathrm{Int}_K(A_P)$. □

Example 3.6. Corollary 3.5 can be applied when $D = \mathbb{Z}$ and A is a certain quaternion algebra. Let $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ be such that $\mathbf{i}^2 = \mathbf{j}^2 = -1$ and $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$. Let A be either the Lipschitz quaternions

$$A = \{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \mid a_i \in \mathbb{Z}\}$$

or the Hurwitz quaternions

$$A = \{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \mid a_i \in \mathbb{Z} \text{ for all } i \text{ or } a_i \in \mathbb{Z} + \tfrac{1}{2} \text{ for all } i\}.$$

In either case, it is a standard exercise (cf. [14, Exer. 3A]) that for each odd prime p and each $k > 0$, we have $A/p^kA \cong M_2(\mathbb{Z}/p^k\mathbb{Z})$. Hence, Corollary 3.5 applies, and the polynomial F from Construction 2.1 is properly integral over $\mathrm{Int}_{\mathbb{Q}}(A)$.

In particular, consider the polynomial F obtained when $p = 3$. The numerator of F is

$$G(x) = x(x^2+3)(x^2+6)(x-1)((x-1)^2+3)((x-1)^2+6) \\ \times (x-2)((x-2)^2+3)((x-2)^2+6)(x^2+1)^3(x^2+x+2)^3(x^2+2x+2)^3$$

and $F(x) = G(x)/27$, a polynomial of degree 33 that is properly integral over $\mathrm{Int}_{\mathbb{Q}}(A)$.

By contrast, a polynomial $g(x)/27 \in \mathrm{Int}_{\mathbb{Q}}(A)$ (with $g(x) \in \mathbb{Z}[x]$ not divisible by 3) must have degree at least 36. Indeed, the isomorphisms $A/3^kA \cong M_2(\mathbb{Z}/3^k\mathbb{Z})$, $k \in \mathbb{N}$, imply that a polynomial $g_1(x)/3^{k_1}$ (with $g_1 \in \mathbb{Z}[x]$ not divisible by 3, and $k_1 > 0$) is in $\mathrm{Int}_{\mathbb{Q}}(A)$ if and only if it is in $\mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}))$. As our results in Section 4 (such as Corollary 4.20) will show, if $g(x)/27 \in \mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}))$, then $\deg(g) \geq 36$. Explicitly, $[(x^9-x)(x^3-x)]^3/27 \in \mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}))$ (and hence is in $\mathrm{Int}_{\mathbb{Q}}(A)$ as well), and there is no polynomial of the form $g(x)/27$ of smaller degree in $\mathrm{Int}_{\mathbb{Q}}(A)$.

4. Null ideals and π-sequences

Maintain the notation given at the start of Section 2. Our work so far shows that the polynomial F from Construction 2.1 is properly integral over $\mathrm{Int}_K(M_n(V))$. However, it is possible that there could be a polynomial of degree less than F that is also properly integral over $\mathrm{Int}_K(M_n(V))$. This inspires the next definition.

Definition 4.1. Let V be a DVR with fraction field K. A polynomial $f \in K[x]$ that is properly integral over $\mathrm{Int}_K(M_n(V))$ is said to be *optimal* if f is of minimal degree among all properly integral polynomials over $\mathrm{Int}_K(M_n(V))$.

We are interested in determining whether our polynomial F is optimal. In general, this is quite hard to do. One way to make progress is to follow the lead of [9] and study P-sequences for $\mathrm{Int}_K(M_n(V))$ and $\mathrm{Int}_K(\Lambda_n(V))$.

Bhargava introduced P-sequences and P-orderings for Dedekind domains in [4], and these notions were extended to certain noncommutative rings by Johnson in [15]. Among other uses, P-sequences and P-orderings can be used to give regular bases for rings of integer-valued polynomials (see [4,15], and [9]). For our purposes, P refers to the maximal ideal πV of V, and we will consider π-sequences for $\mathrm{Int}_K(M_n(V))$ and $\mathrm{Int}_K(\Lambda_n(V))$.

Recall first Johnson's definition from [15], and its connection to integer-valued polynomials.

Definition 4.2. ([15, Def. 1.1]) Let K be a local field with valuation v, D a division algebra over K to which the valuation v extends, R the maximal order in D, and S a subset of R. Then, a *v-ordering* of S is a sequence $\{a_i \mid i \in \mathbb{N}\} \subseteq S$ with the property that for each $i > 0$ the element a_i minimizes the quantity $v(f_i(a_0,\dots,a_{i-1})(a))$ over $a \in S$, where $f_0 = 1$ and, for $i > 0$, $f_i(a_0,\dots,a_{i-1})(x)$ is the minimal polynomial (in the sense of [16]) of the set $\{a_0, a_1, \dots, a_{i-1}\}$. The sequence of valuations $\{v(f_i(a_0,\dots,a_{i-1})(a_i)) \mid i \in \mathbb{N}\}$ is called the *v-sequence* of S.

Proposition 4.3. *([15, Prop. 1.2]) With notation as in Definition 4.2, let $\pi \in R$ be a uniformizing element. Then, the v-sequence $\{\alpha_S(i) = v(f_i(a_0, \ldots, a_{i-1})(a_i)) \mid i \in \mathbb{N}\}$ depends only on the set S and not on the choice of v-ordering. Moreover, the sequence of polynomials*

$$\{\pi^{-\alpha_S(i)} f_i(a_0, \ldots, a_{i-1})(x) \mid i \in \mathbb{N}\}$$

forms a regular R-basis for the R-algebra of polynomials integer-valued on S.

In [9], Evrard and Johnson used these notions to construct p-sequences (p a prime of $\mathbb{Z}$) and regular bases for $\mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}_{(p)}))$ and its integral closure $\mathrm{Int}_{\mathbb{Q}}(R_{2,p})$ (here, $R_{2,p}$ is the maximal order of a division algebra of degree 4 over the field of p-adic numbers). We take a slightly different approach and define our π-sequences with regular bases and optimal polynomials in mind.

Definition 4.4. Express polynomials in $K[x]$ in lowest terms, i.e. in the form $g(x)/\pi^k$, where $g \in V[x]$, $k \geq 0$, and, if $k > 0$, then π does not divide g. The π-sequence $\mu_0, \mu_1, \ldots$ of $\mathrm{Int}_K(M_n(V))$ is the sequence of non-negative integers such that

$$\mu_d = \max\{k \mid \text{ there exists } g_d(x)/\pi^k \in \mathrm{Int}_K(M_n(V)) \text{ of degree } d\}.$$

In other words, having $\mu_d = k$ means there exists $g_d(x) \in V[x]$ of degree d such that $g_d(x)/\pi^k \in \mathrm{Int}_K(M_n(V))$ with k as large as possible.

The π-sequence $\lambda_0, \lambda_1, \ldots$ of $\mathrm{Int}_K(\Lambda_n(V))$ is defined similarly.

Lemma 4.5. *For each $d \in \mathbb{N}$, let f_d be a polynomial of degree d in $V[x] \setminus \pi V[x]$, and let α_d be a non-negative integer. If $\{f_d(x)/\pi^{\alpha_d} \mid d \in \mathbb{N}\}$ is a regular V-basis for $\mathrm{Int}_K(M_n(V))$ (respectively, $\mathrm{Int}_K(\Lambda_n(V))$), then $\mu_d = \alpha_d$ (respectively, $\lambda_d = \alpha_d$) for all d.*

Proof. We will prove this for $\mathrm{Int}_K(M_n(V))$ and μ_d; the proof for $\mathrm{Int}_K(\Lambda_n(V))$ and λ_d is identical. By means of the notion of characteristic ideals and using [5, Prop. II.1.4], the sequence $\{g_d(x)/\pi^{\mu_d} \mid d \in \mathbb{N}\}$ forms a regular V-basis for $\mathrm{Int}_K(M_n(V))$. Let $\{f_d(x)/\pi^{\alpha_d} \mid d \in \mathbb{N}\}$ be another regular V-basis for $\mathrm{Int}_K(M_n(V))$. Then, we must have $\mu_d = \alpha_d$, because the leading coefficients of the elements of two regular bases of the same degree must have the same valuation. □

Relating the previous definition and lemma to the work done in [9], we obtain the following.

Corollary 4.6. *Let $n = 2$, let p be a prime of $\mathbb{Z}$, and let $V = \mathbb{Z}_{(p)}$. Then, λ_d is equal to the p-sequence for $\mathrm{Int}_{\mathbb{Q}}(R_{2,p})$ given in [9, Cor. 2.17].*

Returning now to the question of optimal properly integral polynomials, we can phrase things in terms of π-sequences. Since $\mathrm{Int}_K(M_n(V)) \subsetneq \mathrm{Int}_K(\Lambda_n(V))$, we have $\mu_d \leq \lambda_d$

for all d, and there exists d such that $\mu_d < \lambda_d$. Assume we have found the smallest d such that $\mu_d < \lambda_d$. Then, there exists a properly integral polynomial $f(x) = g(x)/\pi^{\lambda_d}$ of degree d, and $f(x)$ is optimal.

By Corollary 4.6, when $n = 2$ and p is a prime of $\mathbb{Z}$, the terms of λ_d can be computed by using recursive formulas given in [9]. For the general case where $n \geq 2$ and V is a DVR, we now proceed to use the null ideals of the matrix rings $M_n(V/\pi^k V)$ to compute the initial terms of μ_d, although we will not be able to give a formula for the complete sequence. Nevertheless, we will be able to prove (Corollary 4.21) that the properly integral polynomial F constructed for $\mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}_{(p)}))$ is optimal.

We first recall the definition of a null ideal.

Definition 4.7. Let R be a commutative ring, and let S be a subset of some ring containing R. We define the *null ideal* of S in R to be $N_R(S) = \{f \in R[x] \mid f(S) = 0\}$.

There is a strong connection between null ideals and integer-valued polynomials, as described in the next lemma. This relationship has been used before in various forms (see [13,18,23], and [25], for example).

Lemma 4.8. *In the above notation, let $k \in \mathbb{N}$ and $f(x) = g(x)/\pi^k \in K[x]$, for some $g \in V[x]$. Then $f(x)$ is in $\mathrm{Int}_K(M_n(V))$ if and only if $g(x)$ mod π^k is in $N_{V/\pi^k V}(M_n(V/\pi^k V))$.*

Proof. The polynomial $f(x)$ is integer-valued over $M_n(V)$ if and only if $g(x)$ maps every matrix in $M_n(V)$ to the ideal $\pi^k M_n(V) = M_n(\pi^k V)$. Considering everything modulo $\pi^k V$, we get the stated result, using the fact that $M_n(\pi^k V) \cap V = \pi^k V$. $\square$

Hence, null ideals can give us information about rings of integer-valued polynomials. We are interested in describing generators for the null ideal of $M_n(V/\pi^k V)$ in $V/\pi^k V$. The following polynomials will be crucial in our treatment.

Notation 4.9. For each $n \geq 1$ and each prime power q, we define

$$\Phi_{q,n}(x) = (x^{q^n} - x)(x^{q^{n-1}} - x) \cdots (x^q - x).$$

With a slight abuse of notation, we will use $\Phi_{q,n}(x)$ to denote the same polynomial over any of the residue rings $V/\pi^k V$, $k \in \mathbb{N}$. The coefficient ring of the polynomial will be clear from the context.

Our goal for most of the rest of this section is to prove the next theorem.

Theorem 4.10. *Let $n \geq 1$ and let $1 \leq k \leq q$. Then,*

$$N_{V/\pi^k V}(M_n(V/\pi^k V)) = (\Phi_{q,n}(x), \pi)^k = (\Phi_{q,n}(x)^k, \pi\Phi_{q,n}(x)^{k-1}, \ldots, \pi^{k-1}\Phi_{q,n}(x)).$$

Using different terminology, this theorem was proven for $k = 1$ in [3, Thm. 3]; we will revisit that result below in Theorem 4.14. When $n = 1$, we have $\Phi_{q,1}(x) = x^q - x$, and Theorem 4.10 is the assertion that $N_{V/\pi^k V}(V/\pi^k V) = (x^q - x, \pi)^k$ for $1 \leq k \leq q$. If, in addition, V is a localization of $\mathbb{Z}$, then this is actually a classical result which can be found in the book of Dickson [7, Thm. 27, p. 22]. An alternate modern treatment, which examines the pullback to $\mathbb{Z}[x]$ of the null ideal $N_{\mathbb{Z}/p^k\mathbb{Z}}(\mathbb{Z}/p^k\mathbb{Z})$, is given in [19, Thm. 3.1].

The proof of Theorem 4.10 is complicated, and involves several stages and preliminary results. We will need to work with different sets of polynomial, common multiples, and least common multiples across the different residue rings $V/\pi^k V$. To help simplify the necessary notation, we adopt the following conventions (the need for all this notation will become apparent as we work through the proof).

Definitions–Notations 4.11.

- For each $k \geq 1$ let $V_k = V/\pi^k V$ and $N_k = N_{V_k}(M_n(V_k))$. Note that $V_1 = \mathbb{F}_q$.
- Since n and q will be fixed, let $\Phi = \Phi_{q,n}$.
- For each $k \geq 1$, let $\phi_k(x)$ be a monic polynomial of minimal degree in N_k.
- For each $k \geq 1$ and each $d \geq 1$, let $\mathcal{P}_d(V_k)$ denote the set of monic polynomials of degree d in $V_k[x]$.
- Let $\mathcal{P}^{\text{irr}}_{\leq n}(\mathbb{F}_q) = \mathcal{P}^{\text{irr}}_{\leq n}$ denote the set of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree at most n.
- For each $k \geq 1$, $f \in V_k[x]$, and $\iota \in \mathcal{P}^{\text{irr}}_{\leq n}$, we say that f is ι-primary if f is monic and the residue of f in $\mathbb{F}_q[x]$ is a positive power of ι.
- For each $k \geq 1$, each $d \geq 1$, and each $\iota \in \mathcal{P}^{\text{irr}}_{\leq n}$, let $\mathcal{P}^{\iota}_d(V_k)$ denote the set of ι-primary polynomials in $V_k[x]$ of degree d.
- For each $k \geq 1$, each $d \geq 1$, and each $\iota \in \mathcal{P}^{\text{irr}}_{\leq n}$, let $L^{\iota}_d(V_k)$ be a monic least common multiple (lcm) for the polynomials in $\mathcal{P}^{\iota}_d(V_k)$. That is, $L^{\iota}_d(V_k)$ is a monic polynomial in $V_k[x]$ of least degree such that each $f \in \mathcal{P}^{\iota}_d(V_k)$ divides $L^{\iota}_d(V_k)$. An lcm need not be unique but the degree of an lcm is uniquely determined (see the discussion in [24]).

In [13], Frisch described some general properties of null ideals and matrices that we will find very useful.

Lemma 4.12.

(1) *[13, Lem. 3.3] Let R be a commutative ring, $f \in R[x]$ a monic polynomial and $C \in M_n(R)$ the companion matrix of f. Then $N_R(C) = f(x)R[x]$.*

(2) *[13, Lem. 3.4] Let D be a domain and $f(x) = g(x)/c$, $g \in D[x]$, $c \in D \setminus \{0\}$. Then $f \in \text{Int}_K(M_n(D))$ if and only if g is divisible modulo $cD[x]$ by all monic polynomials in $D[x]$ of degree n.*

Specializing to our situation, we easily obtain the following corollary.

Corollary 4.13. *Let $k \geq 1$.*

(1) *Let $f \in V_k[x]$, let $m \in \mathcal{P}_n(V_k)$, and let $C \in M_n(V_k)$ be the companion matrix for m. Then, m divides f if and only if $f(C) = 0$.*
(2) *Let $f \in V_k[x]$. Then, $f \in N_k$ if and only if f is divisible by every polynomial in $\mathcal{P}_n(V_k)$.*
(3) *The polynomial ϕ_k is an lcm for $\mathcal{P}_n(V_k)$.*

Proof. Part (1) is a restatement of Lemma 4.12 (1). Part (2) follows from Lemmas 4.8 and 4.12 (2). Finally, for (3), ϕ_k is monic by assumption, and is a common multiple for $\mathcal{P}_n(V_k)$ because $\phi \in N_k$. But, the minimality of $\deg \phi_k$ means that ϕ_k is in fact an lcm for $\mathcal{P}_n(V_k)$. $\square$

Thus, we have established a connection between null ideals and least common multiples of the sets $\mathcal{P}_n(V_k)$. If we focus on the case $k = 1$, then everything is taking place over the field $\mathbb{F}_q$. In this situation, the aforementioned theorem [3, Thm. 3] brings us back to the polynomial $\Phi = \Phi_{q,n}$.

Theorem 4.14. *([3, Thm. 3 & eq. (3.3)]) Let $n \geq 1$ and let q be a prime power. Let $\Phi_{q,n}$ be as in Notation 4.9.*

(1) *$N_{\mathbb{F}_q}(M_n(\mathbb{F}_q))$ is generated by $\Phi_{q,n}$.*
(2) *$\Phi_{q,n}$ is the (unique) lcm for $\mathcal{P}_n(\mathbb{F}_q)$.*
(3) *The factorization of $\Phi_{q,n}$ into irreducible polynomials is*

$$\Phi_{q,n} = \prod_{\iota \in \mathcal{P}^{\mathrm{irr}}_{\leq n}} \iota^{\lfloor n/\deg \iota \rfloor}.$$

Finally, we have all the necessary tools and can proceed with the proof of Theorem 4.10. We break the proof up into three Claims. The first claim shows that it suffices to compare the degrees of the polynomials ϕ_k and Φ^k.

Claim 1. To prove Theorem 4.10, it suffices to show that $\deg(\phi_k) \geq \deg(\Phi^k)$ for all $1 \leq k \leq q$.

Proof. Fix k between 1 and q. Since over $\mathbb{F}_q$ we have $N_1 = (\Phi)$ by Theorem 4.14 (1), over V_k we have $\Phi^k \in N_k$, and by [25, Thm. 5.4], the ideal N_k is equal to $(\phi_k, \pi\phi_{k-1}, \pi^2\phi_{k-2}, \ldots, \pi^{k-1}\phi_1)$. So, to prove Theorem 4.10, it will be enough to show that we can take $\phi_k = \Phi^k$, and doing so is valid if $\deg(\phi_k) = \deg(\Phi^k)$.

Now, by Corollary 4.13 part (3), ϕ_k is an lcm for $\mathcal{P}_n(V_k)$. We will show that Φ^k is a common multiple for $\mathcal{P}_n(V_k)$, i.e. that each $f \in \mathcal{P}_n(V_k)$ divides Φ^k. To do this, let $f \in \mathcal{P}_n(V_k)$ and let $C \in M_n(V_k)$ be the companion matrix for f.

Recall that we have a canonical projection map from $M_n(V_k)$ to $M_n(\mathbb{F}_q)$, whose kernel is $\pi M_n(V_k) = M_n(\pi V_k)$. Over the residue field $\mathbb{F}_q$, by Theorem 4.14 the polynomial Φ is zero on the matrix obtained by reducing the entries of C modulo π. It follows that over V_k we have $\Phi(C) \in M_n(\pi V_k)$. Hence, $\Phi(C)^k = 0$ in $M_n(V_k)$.

By Corollary 4.13 (1), f divides Φ^k, and since f was arbitrary, we conclude that Φ^k is a common multiple for $\mathcal{P}_n(V_k)$. Since ϕ_k is an lcm for $\mathcal{P}_n(V_k)$, we have $\deg(\phi_k) \le \deg(\Phi^k)$. Thus, to complete the proof, it suffices to show that $\deg(\phi_k) \ge \deg(\Phi^k)$. $\square$

Next, we argue that it is enough just to focus our attention on ι-primary polynomials.

Claim 2. To prove Theorem 4.10, it suffices to show that for all $1 \le k \le q$ and all $\iota \in \mathcal{P}^{\mathrm{irr}}_{\le n}$, we have $\deg(L^\iota_D(V_k)) \ge kD$, where $D = \deg(\iota)\lfloor \frac{n}{\deg(\iota)} \rfloor$.

Proof. Let $D = \deg(\iota)\lfloor \frac{n}{\deg(\iota)} \rfloor$. By Theorem 4.14 (3), we have

$$\Phi^k = \prod_{\iota \in \mathcal{P}^{\mathrm{irr}}_{\le n}} \iota^{k\lfloor n/\deg \iota \rfloor}. \tag{4.15}$$

Moreover, by [24, Thm. 5.1] we know that the polynomial $\prod_{\iota \in \mathcal{P}^{\mathrm{irr}}_{\le n}} L^\iota_D(V_k)$ is an lcm for $\mathcal{P}_n(V_k)$. Thus, we can take

$$\phi_k = \prod_{\iota \in \mathcal{P}^{\mathrm{irr}}_{\le n}} L^\iota_D(V_k). \tag{4.16}$$

Comparing (4.15) and (4.16) gives us a method of attack: we can prove that $\deg(\phi_k) \ge \deg(\Phi^k)$ by showing that for each ι, we have

$$\deg(L^\iota_D(V_k)) \ge \deg(\iota^{k\lfloor n/\deg \iota \rfloor}) = k\deg(\iota)\lfloor \tfrac{n}{\deg(\iota)} \rfloor = kD. \quad \square \tag{4.17}$$

To complete the proof of Theorem 4.10, all that remains is to justify the inequality (4.17) from the previous claim.

Claim 3. Let $1 \le k \le q$ and let $\iota \in \mathcal{P}^{\mathrm{irr}}_{\le n}$. Let $D = \deg(\iota)\lfloor \frac{n}{\deg(\iota)} \rfloor$. Then, $\deg(L^\iota_D(V_k)) \ge kD$.

Proof. For the final stage of the proof, k and ι are fixed, so we can simplify the notation. Let $d = \deg \iota$, let $D = d\lfloor \frac{n}{d} \rfloor$, let $\mathcal{P} = \mathcal{P}^\iota_D(V_k)$, and let $f = L^\iota_D(V_k)$. We need to prove that $\deg f \ge kD$. Unless stated otherwise, calculations take place mod π^k.

Choose a k-element subset $\{a_1, \dots, a_k\}$ from $\mathbb{F}_q$. For each $1 \le j \le k$, let $m_j(x) = (\iota(x))^{\lfloor n/d \rfloor} - \pi a_j \in \mathcal{P}$, and let $C_j \in M_D(V_k)$ be the $D \times D$ companion matrix for m_j.

Then, for all $1 \le j \le k$, we have $m_j(C_j) = 0$ and $(\iota(C_j))^{\lfloor n/d \rfloor} = \pi a_j I$. This latter relation implies that $m_j(C_{j'}) = \pi(a_{j'} - a_j)I$ for all $1 \le j, j' \le k$.

Now, m_1 divides f because f is an lcm for $\mathcal{P}$. Since both m_1 and f are monic, there exists a monic $f_1 \in V_k[x]$ such that $f = m_1 f_1$. If $k = 1$, then we are done, so assume that $k \ge 2$. In that case, m_2 also divides f, so

$$0 = f(C_2) = m_1(C_2) f_1(C_2) = \pi(a_2 - a_1) f_1(C_2).$$

This equality occurs mod π^k, and $a_2 - a_1$ is a unit mod π (hence is a unit mod π^k), so $f_1(C_2) \equiv 0 \bmod \pi^{k-1}$. Thus, m_2 divides f_1 mod π^{k-1}, so in $V_k[x]$ we may write $f_1 = m_2 f_2 + \pi^{k-1} g_1$, where $f_2, g_1 \in V_k[x]$, f_2 is monic, and $\deg g_1 < \deg f_1 = \deg f - D$.

At this point, we have

$$f = m_1 f_1 = m_1(m_2 f_2 + \pi^{k-1} g_1) = m_1 m_2 f_2 + \pi^{k-1} m_1 g_1.$$

If $k = 2$, we are done; if not, applying the same argument as above yields

$$\begin{aligned} 0 &= f(C_3) \\ &= m_1(C_3) m_2(C_3) f_2(C_3) + \pi^{k-1} m_1(C_3) g_1(C_3) \\ &= \pi^2 (a_3 - a_1)(a_3 - a_2) f_2(C_3) + 0. \end{aligned}$$

Since $(a_3 - a_1)(a_3 - a_2)$ is a unit mod π^k, we have $f_2(C_3) \equiv 0 \bmod \pi^{k-2}$. The same steps as before will give us

$$f = m_1 m_2 m_3 f_3 + \pi^{k-1} m_1 g_1 + \pi^{k-2} m_1 m_2 g_2$$

where $f_3, g_2 \in V_k[x]$, f_3 is monic, and $\deg g_2 < \deg f_2 = \deg f - 2D$.

Since $k \le q$, the product $(a_k - a_1)(a_k - a_2) \cdots (a_k - a_{k-1})$ will always be a unit mod π^k. Thus, we can continue this process as long as necessary, ultimately resulting in the expansion

$$f = m_1 m_2 \cdots m_k f_k + \pi g$$

where $f_k, g \in V_k[x]$, f_k is monic, and $\deg g < \deg f$. Since each m_j has degree D, we conclude that $\deg f \ge kD$, as required. $\square$

Remark 4.18. Theorem 4.10 does not hold once $k > q$; we demonstrate this by example below. Examining the proof gives some indication why. The final stage of the proof relied on the fact that the product $(a_k - a_1)(a_k - a_2) \cdots (a_k - a_{k-1})$ is nonzero mod π, and this will not be true once $k > q$. Products of this form arise naturally with P-orderings [4], and illustrate once again the close connections between P-orderings and integer-valued polynomials.

Example 4.19. Theorem 4.10 is false for $k = q + 1$. Let

$$\begin{aligned}
\theta(x) &= \Phi/\Big(\prod_{a\in\mathbb{F}_q}(x-a)^n\Big) = \prod_{\iota\in\mathcal{P}^{\mathrm{irr}}_{\leq n},\deg\iota\geq 2} \iota(x)^{\lfloor n/\deg\iota\rfloor},\\
\ell(x) &= x^{n-1}\prod_{a\in\mathbb{F}_q}(x^n+\pi a),\\
L(x) &= \prod_{a\in\mathbb{F}_q}\ell(x-a), \text{ and}\\
\psi(x) &= L(x)\theta(x)^{q+1}
\end{aligned}$$

(cf. Construction 2.1). We claim that $\psi \in N_{q+1}$. Let C be the companion matrix for a polynomial $m \in \mathcal{P}_n(V_{q+1})$. If $m \not\equiv (x-a)^n \bmod \pi$ for all $a \in \mathbb{F}_q$, then $\theta(C) \equiv 0 \bmod \pi$, so $\psi(C) \equiv 0 \bmod \pi^{q+1}$. So, assume $m \equiv (x-a)^n \bmod \pi$ for some $a \in \mathbb{F}_q$.

Assume first that $a = 0$, and consider $m \bmod \pi^2$. There exists $b \in \mathbb{F}_q$ such that the constant term of m is equivalent to $-\pi b \bmod \pi^2$. Consequently, $C^n + \pi bI$ is divisible by $\pi C \bmod \pi^2$. It follows that $C^{n-1}(C^n + \pi bI) \equiv 0 \bmod \pi^2$, and so $\ell(C) \equiv 0 \bmod \pi^{q+1}$. By translation, $L(C) \equiv 0 \bmod \pi^{q+1}$ regardless of the choice of a. We conclude that $\psi(C) \equiv 0 \bmod \pi^{q+1}$ for all companion matrices C. Thus, $\psi \in N_{q+1}$.

However, one may compute that $\deg\psi = (q+1)\deg\Phi - q$. Since $\deg\phi_{q+1} \leq \deg\psi < \deg(\Phi^{q+1})$, Theorem 4.10 does not hold for $k = q + 1$.

We close the paper by once again considering π-sequences and optimal polynomials (see the definitions given at the start of this section). By using Theorem 4.10, we can give a succinct formula for the initial terms of the π-sequence μ_d.

Corollary 4.20. *The π-sequence μ_d for $\mathrm{Int}_K(M_n(V))$ satisfies $\mu_d = \lfloor d/\deg\Phi_{q,n}\rfloor$ for $0 \leq d \leq q\cdot\deg\Phi_{q,n}$.*

Proof. The polynomial $g(x)/\pi^k \in K[x]$ (where $g \in V[x]$ and π does not divide g) is in $\mathrm{Int}_K(M_n(V))$ if and only if $g(x) \bmod \pi^k$ is in the null ideal N_k (Lemma 4.8). Moreover, μ_d is equal to the maximum k such that there exists $g(x)/\pi^k \in \mathrm{Int}_K(M_n(V))$ of degree d. It follows that, for any $k > 0$, we have $\mu_{\deg\phi_k} = k$, and $\mu_d < k$ for $d < \deg\phi_k$. By Theorem 4.10, $\deg\phi_k = k\deg\Phi_{q,n}$ for $1 \leq k \leq q$. Hence, the sequence μ_d begins

$$\underbrace{0,\dots,0}_{\deg\Phi_{q,n}\text{ terms}},\ \underbrace{1,\dots,1}_{\deg\Phi_{q,n}\text{ terms}},\ \dots,\ \underbrace{q-1,\dots,q-1}_{\deg\Phi_{q,n}\text{ terms}},\ q,$$

which matches the stated formula. □

In general, it is harder to describe the π-sequence λ_d of $\mathrm{Int}_K(\Lambda_n(V))$. Thankfully, formulas for the case $n = 2$ and $V = \mathbb{Z}_{(p)}$ are given in [9], and we can use these to show that our polynomial F is optimal in that case.

Corollary 4.21. *Let p be a prime of* $\mathbb{Z}$*. Then, the polynomial F given by Construction 2.1 for* $\mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}_{(p)}))$ *is optimal.*

Proof. The degree of $\Phi_{p,2}$ is p^2+p, so Corollary 4.20 tells us that the p-sequence μ_d of $\mathrm{Int}_{\mathbb{Q}}(M_2(\mathbb{Z}_{(p)}))$ satisfies $\mu_d = \lfloor d/(p^2+p)\rfloor$ for $0 \le d \le p^3+p^2$. The p-sequence λ_d of $\mathrm{Int}_{\mathbb{Q}}(\Lambda_2(\mathbb{Z}_{(p)}))$ can be computed via recursive formulas given in [9, Prop. 2.13, Prop. 2.10, Cor. 2.17]. An elementary, but tedious, calculation (which we omit for the sake of space) shows that for $0 \le d < p^3+p^2-p$, we have $\lambda_d = \lfloor d/(p^2+p)\rfloor < p$, and $\lambda_{p^3+p^2-p} = p$. Thus, the smallest d for which $\mu_d < \lambda_d$ is $d = p^3+p^2-p$. A routine computation shows that $\deg F = p^3+p^2-p$, so we conclude that F is optimal. □

It is an open problem to determine whether Corollary 4.21 holds in the general case.

Question 4.22. Let V be a DVR with fraction field K and residue field $\mathbb{F}_q$, and let $n \ge 2$. Is the polynomial F given by Construction 2.1 optimal? To prove this, it would suffice to show that $\lambda_d = \mu_d$ for all $d < \deg F = q\deg\Phi_{q,n} - q$. We will not include the proof, but we have been able to determine that $\lambda_d = \mu_d = 0$ for $0 \le d < \deg\Phi_{q,n}$. However, we have not been able to prove that equality holds for larger d (although we suspect that this is the case).

Acknowledgments

This research has been supported by the grant "Bando Giovani Studiosi 2013", Project title "Integer-valued polynomials over algebras", Prot. GRIC13X60S of the University of Padova. The authors wish to thank the referee for several suggestions which improved the paper.

References

[1] M.F. Atiyah, I.G. MacDonald, Introduction to Commutative Algebra, Addison–Wesley Publishing Co., Reading, MA, 1969.
[2] N. Bourbaki, Commutative Algebra, Hermann/Addison-Wesley Publishing Co., Paris/Reading, Mass., 1972.
[3] J.V. Brawley, L. Carlitz, J. Levine, Scalar polynomial functions on the $n \times n$ matrices over a finite field, Linear Algebra Appl. 10 (1975) 199–217.
[4] M. Bhargava, *P*-orderings and polynomial functions on arbitrary subsets of Dedekind rings, J. Reine Angew. Math. 490 (1997) 101–127.
[5] P.-J. Cahen, J.-L. Chabert, Integer-Valued Polynomials, Mathematical Surveys and Monographs, vol. 48, Amer. Math. Soc., Providence, 1997.
[6] J.-L. Chabert, G. Peruginelli, Polynomial overrings of $\mathrm{Int}(\mathbb{Z})$, J. Commut. Algebra 8 (1) (2016) 1–28.
[7] L.E. Dickson, Introduction to the Theory of Numbers, Univ. Chicago Press, Chicago, 1929.
[8] S. Evrard, Y. Fares, K. Johnson, Integer valued polynomials on lower triangular integer matrices, Monatsh. Math. 170 (2) (2013) 147–160.
[9] S. Evrard, K. Johnson, The ring of integer-valued polynomials on 2×2 matrices and its integral closure, J. Algebra 441 (2015) 660–677.
[10] S. Frisch, Integer-valued polynomials on algebras, J. Algebra 373 (2013) 414–425.

[11] S. Frisch, Corrigendum to "Integer-valued polynomials on algebras" [J. Algebra 373 (2013) 414–425], J. Algebra 412 (2014) 282.

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

[13] S. Frisch, Polynomial separation of points in algebras, in: Arithmetical Properties of Commutative Rings and Monoids, in: Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall, Boca Raton, FL, 2005.

[14] K. Goodearl, R. Warfield Jr., An Introduction to Noncommutative Noetherian Rings, London Mathematical Society, Student Texts, vol. 16, Cambridge University Press, Cambridge, 2004.

[15] K. Johnson, P-orderings of noncommutative rings, Proc. Amer. Math. Soc. 143 (8) (2015) 3265–3279.

[16] T.Y. Lam, A. Leroy, Wedderburn polynomials over division rings. I, J. Pure Appl. Algebra 186 (1) (2004) 43–76.

[17] K.A. Loper, N.J. Werner, Generalized rings of integer-valued polynomials, J. Number Theory 132 (11) (2012) 2481–2490.

[18] G. Peruginelli, Integer-valued polynomials over matrices and divided differences, Monatsh. Math. 173 (4) (2014) 559–571.

[19] G. Peruginelli, Primary decomposition of the ideal of polynomials whose fixed divisor is divisible by a prime power, J. Algebra 398 (2014) 227–242.

[20] G. Peruginelli, The ring of polynomials integral-valued over a finite set of integral elements, J. Commut. Algebra 8 (1) (2016) 113–141.

[21] G. Peruginelli, Integral-valued polynomials over sets of algebraic integers of bounded degree, J. Number Theory 137 (2014) 241–255.

[22] G. Peruginelli, N.J. Werner, Integral closure of rings of integer-valued polynomials on algebras, in: M. Fontana, S. Frisch, S. Glaz (Eds.), Commutative Algebra: Recent Advances in Commutative Rings, Integer-Valued Polynomials, and Polynomial Functions, Springer, ISBN 978-1-4939-0924-7, 2014, pp. 293–305.

[23] N.J. Werner, Int-decomposable algebras, J. Pure Appl. Algebra 218 (10) (2014) 1806–1819.

[24] N.J. Werner, On least common multiples of polynomials in $\mathbb{Z}/n\mathbb{Z}[x]$, Comm. Algebra 40 (6) (2012) 2066–2080.

[25] N.J. Werner, Polynomials that kill each element of a finite ring, J. Algebra Appl. 13 (3) (2014).