

INTEGER-VALUED POLYNOMIALS ON ALGEBRAS

Sophie Frisch

frisch@TUGraz.at

ABSTRACT. Let D be a domain with quotient field K and A a D -algebra. A polynomial with coefficients in K that maps every element of A to an element of A is called integer-valued on A . For commutative A we also consider integer-valued polynomials in several variables. For an arbitrary domain D and I an arbitrary ideal of D we show I -adic continuity of integer-valued polynomials on A . For Noetherian one-dimensional D , we determine spectrum and Krull dimension of the ring $\text{Int}_D(A)$ of integer-valued polynomials on A . We do the same for the ring of polynomials with coefficients in $M_n(K)$, the K -algebra of $n \times n$ matrices, that map every matrix in $M_n(D)$ to a matrix in $M_n(D)$.

2000 MSC: Primary 13F20; Secondary 16S50, 13B25, 13J10, 11C08, 11C20.

1. Introduction

Let D be a domain with quotient field K and A a D -algebra, such as, for instance, a group ring $D(G)$ or the matrix algebra $M_n(D)$.

We are interested in the rings of polynomials

$$\text{Int}_D(A) = \{f \in K[x] \mid f(A) \subseteq A\},$$

and, if A is commutative,

$$\text{Int}_D^n(A) = \{f \in K[x_1, \dots, x_n] \mid f(A^n) \subseteq A\}.$$

Elements of the D -algebra A are plugged into polynomials with coefficients in K via the canonical homomorphism $\iota_A : A \rightarrow K \otimes_D A$, $\iota_A(a) = 1 \otimes a$.

In the special case $A = D$ these rings are known as rings of integer-valued polynomials, cf. [3]. They provide natural examples of non-Noetherian Prüfer rings [5, 11], and have been used for proving results on the n -generator property in Prüfer rings [2]. Also, integer-valued polynomials are useful for polynomial

interpolation of functions from D to D [8, 4], and satisfy other interesting algebraic conditions such as analogues of Hilbert’s Nullstellensatz [3, 9].

These desirable properties of rings of integer-valued polynomials have motivated the generalization to polynomials with coefficients in K acting on a D -algebra A [10, 12]. So far, not much is known about rings of integer-valued polynomials on algebras. We know that they behave somewhat like the classical rings of integer-valued polynomials if the D -algebra A is commutative. For instance, Loper and Werner [12] have shown that $\text{Int}_{\mathbb{Z}}(\mathcal{O}_K)$ is Prüfer. If A is non-commutative, however, the situation is radically different. For instance, $\text{Int}_{\mathbb{Z}}(M_2(\mathbb{Z}))$ is not Prüfer [12], and is far from allowing interpolation [10].

We will describe the spectrum of $\text{Int}_D(A)$, for a one-dimensional Noetherian ring D and a finitely generated torsion-free D -algebra A , in the hope that this will facilitate further research. We will investigate more closely the special case of $A = M_n(D)$: we determine a polynomially dense subset of $M_n(D)$ and describe the image of a given matrix under the ring $\text{Int}_D(M_n(D))$.

A different ring of integer-valued polynomials on the matrix algebra $M_n(D)$, consisting of polynomials with coefficients in $M_n(K)$ that map matrices in $M_n(D)$ to matrices in $M_n(D)$, has been introduced by Werner [13]. We will show that it is isomorphic to the algebra of $n \times n$ matrices over “our” ring $\text{Int}_D(M_n(D))$ of integer-valued polynomials on $M_n(D)$ with coefficients in K .

Before we give a precise definition of the kind of D -algebra A for which we will investigate $\text{Int}_D(A)$, a few examples. D is always a domain with quotient field K , and not a field.

1.1 Example. For fixed $n \in \mathbb{N}$, let $A = M_n(D)$ be the D -algebra of $n \times n$ matrices with entries in D and

$$\text{Int}_D(M_n(D)) = \{f \in K[x] \mid \forall C \in M_n(D) : f(C) \in M_n(D)\}.$$

1.2 Example. Let $H = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ be the \mathbb{Q} -algebra of rational quaternions, $L = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ the \mathbb{Z} -subalgebra of Lipschitz quaternions, and

$$\text{Int}_{\mathbb{Z}}(L) = \{f \in \mathbb{Q}[x] \mid \forall z \in L : f(z) \in L\}.$$

1.3 Example. Let G be a finite group, $K(G)$ and $D(G)$ the respective group rings, and

$$\text{Int}_D(D(G)) = \{f \in K[x] \mid \forall z \in D(G) : f(z) \in D(G)\}.$$

If G is commutative, we also consider

$$\text{Int}_D^n(D(G)) = \{f \in K[x_1, \dots, x_n] \mid \forall z \in D(G)^n : f(z) \in D(G)\}.$$

for $n \in \mathbb{N}$, where $D(G)^n = D(G) \times \dots \times D(G)$ denotes the Cartesian product of n copies of $D(G)$.

1.4 Example. Let $D \subseteq A$ be Dedekind rings with quotient fields $K \subseteq F$, and

$$\text{Int}_D^n(A) = \{f \in K[x_1, \dots, x_n] \mid f(A^n) \subseteq A\}.$$

1.5 Notation and conventions. Throughout this paper, D is a domain and not a field, K the quotient field of D , and A a *torsion-free* D -algebra *finitely generated* as a D -module. Since A is faithful, there is an isomorphic copy of D embedded in A by $d \mapsto d1_A$, and we may assume $D \subseteq A$.

Now let $B = K \otimes_D A$. The natural homomorphisms $\iota_K : K \rightarrow K \otimes_D A$, $\iota_K(k) = k \otimes 1$ and $\iota_A : A \rightarrow K \otimes_D A$, $\iota_A(a) = 1 \otimes a$, are injective, since A is a torsion-free D module. We identify K and A with their isomorphic copies in B , which allows us to evaluate polynomials with coefficients in K at arguments in A , and define

$$\text{Int}_D(A) = \{f \in K[x] \mid \forall a \in A : f(a) \in A\}$$

and for $n \in \mathbb{N}_0$

$$\text{Int}_D^n(A) = \{f \in K[x_1, \dots, x_n] \mid \forall a_1, \dots, a_n \in A : f(a_1, \dots, a_n) \in A\}.$$

To exclude pathological cases we require $K \cap A = D$.

1.6 Remark. Instead of $B = K \otimes_D A$, we could look at the canonically isomorphic $A_{K \setminus \{0\}}$, the ring of fractions of A with denominators in $K \setminus \{0\}$. The natural homomorphisms $\iota_K : K \rightarrow A_{K \setminus \{0\}}$ and $\iota_A : A \rightarrow A_{K \setminus \{0\}}$ then take the form $\iota_K(\frac{c}{d}) = \frac{c1_A}{d}$ and $\iota_A(a) = \frac{a}{1}$.

1.7 Convention regarding polynomials in several variables. For non-commutative A and $n > 1$, $\text{Int}_D^n(A)$ is a priori not closed under multiplication and therefore in general not a ring. With the exception of the following section on I -adic continuity, we will only consider polynomial functions in several variables if the D -algebra A is commutative.

From section 3 onward, statements about $\text{Int}_D^n(A)$ with unspecified n and A are meant as follows: if A is commutative, let $n \in \mathbb{N}_0$, if A is non-commutative, assume $n \leq 1$.

1.8 Remark. Note that $K \cap A = D$ implies

$$\text{Int}_D(A) \subseteq \text{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\}$$

and for commutative A , also

$$\text{Int}_D^n(A) \subseteq \text{Int}(D^n) = \{f \in K[x_1, \dots, x_n] \mid f(D^n) \subseteq D\},$$

and $\text{Int}_D^0(A) = K \cap A = D$.

2. Continuity

I -adic continuity of the function $f: D^n \rightarrow D$ arising from a classical integer-valued polynomial $f \in \text{Int}(D^n) = \{f \in K[x_1, \dots, x_n] \mid f(D^n) \subseteq D\}$ has been shown, for an arbitrary ideal I of an arbitrary domain D , in Prop. 1.4 of [4]. (The proof there is for one variable, but clearly generalizable to several variables.)

To establish I -adic continuity of integer-valued polynomials on algebras, we will briefly look at polynomials in several non-commuting variables. If our algebra A is non-commutative, this becomes necessary, even if we are only interested in integer-valued polynomials in one variable: if we consider $f(x+y) - f(y)$ as a polynomial in two variables, and we still want substitution of elements from A for x and y to be a homomorphism, we must turn to non-commuting variables.

2.1 Definition. Let D be a domain with quotient-field K . Let $K\langle x_1, \dots, x_n \rangle$ be the free associative K -algebra generated by x_1, \dots, x_n (in other words, the semigroup-ring $K(S)$, where S is the free semigroup generated by x_1, \dots, x_n). If A is a torsion-free D -algebra, we evaluate polynomials in $K\langle x_1, \dots, x_n \rangle$ at arguments in $B = K \otimes_D A$ and thus associate a polynomial function $f: B^n \rightarrow B$ to every $f \in K\langle x_1, \dots, x_n \rangle$. Such polynomials as map arguments in A^n to values in A we call integer-valued on A .

From the theory of PID-rings (polynomial identity rings), it is easy to garner non-trivial examples of integer-valued polynomials in several non-commuting variables. For instance, if p is prime and $n \geq 1$, then a polynomial in $\mathbb{Q}\langle x_1, \dots, x_{np} \rangle$, but not in $\mathbb{Z}\langle x_1, \dots, x_{np} \rangle$, that takes every np -tuple of $n \times n$ integer matrices to an integer matrix is

$$f(x_1, \dots, x_{np}) = \frac{1}{p} \sum_{\pi \in S_{np}} x_{\pi(1)} x_{\pi(2)} \dots x_{\pi(np)}.$$

(This follows from [7] or [14].) In this paper, we will not consider polynomials in non-commuting variables except in the following theorem and its corollaries.

2.2 Theorem. *Let D be a domain with quotient-field K and A a torsion-free D -algebra. For every $f \in K\langle x_1, \dots, x_n \rangle$ integer-valued on A , the polynomial function $f: A^n \rightarrow A$ is uniformly I -adically continuous for every ideal I of D .*

Proof. Fix i and let d be the degree of f in x_i . We will show that for every $b \in I^d A$ and every $(a_1, \dots, a_n) \in A^n$,

$$(*) \quad f(a_1, \dots, a_i + b, \dots, a_n) - f(a_1, \dots, a_i, \dots, a_n) \in IA.$$

For $d = 0$, or if f is the zero-polynomial, this is obvious. The polynomial f is uniquely representable as $f = f_1 + f_2$, where x_i doesn't occur in f_1 , x_i occurs in every monomial in the support of f_2 , and f_2 has the same degree in x_i as f . Since $f_1 = f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$ and $f_2 = f - f_1$, both f_1 and f_2 are integer-valued. We can show $(*)$ separately for f_1 and f_2 . As $(*)$ holds for f_1 and arbitrary $b \in A$, we have reduced to the case $f = f_2$, i.e., when x_i occurs in every monomial in the support of f .

Also, it suffices to show $(*)$ for $b = t_d t_{d-1} \dots t_1 c$ with $t_k \in I$ and $c \in A$, because every element of $I^d A$ is a finite sum of elements of this form.

By considering

$$g(x_1, \dots, x_n, z) = f(x_1, \dots, x_i + z, \dots, x_n) - f(x_1, \dots, x_i, \dots, x_n)$$

we can reduce our task to showing for every $g(x_1, \dots, x_n, z) \in K\langle x_1, \dots, x_n, z \rangle$ of degree $d \geq 1$ in z , which maps A^{n+1} to A , satisfies $g(x_1, \dots, x_n, 0) = 0$, and such that z occurs in every monomial in the support of g :

$$(**) \quad g(a_1, \dots, a_n, t_d \dots t_1 c) \in IA \quad \text{whenever} \quad t_1, \dots, t_d \in I \quad \text{and} \quad c \in A.$$

We show $(**)$ by induction on d . Let $d \geq 1$. Consider

$$h(x_1, \dots, x_n, y) = g(x_1, \dots, x_n, t_d y) - t_d^d g(x_1, \dots, x_n, y).$$

h satisfies $h(x_1, \dots, x_n, 0) = 0$, is of degree at most $d - 1$ in y , and y occurs in every monomial in the support of h . Now $h(a_1, \dots, a_n, t_{d-1} \dots t_1 c) \in IA$ for all $t_1, \dots, t_{d-1} \in I$ and $c \in A$, either by induction hypothesis or because h is the zero-polynomial. Therefore $g(a_1, \dots, a_n, t_d t_{d-1} \dots t_1 c) = h(a_1, \dots, a_n, t_{d-1} \dots t_1 c) + t_d^d g(a_1, \dots, a_n, t_{d-1} \dots t_1 c)$ is in IA , for all $t_1, \dots, t_d \in I$ and $c \in A$. \square

Returning to commuting variables, we conclude:

2.3 Corollary. *For any ideal I of D , and every $f \in \text{Int}_D^n(A)$ the function $f: A^n \rightarrow A$ is uniformly I -adically continuous.*

2.4 Corollary. *If M is a maximal ideal of D , \hat{A} the M -adic completion of A , and $f \in \text{Int}_D^n(A)$, then the function $f: A^n \rightarrow A$ defined by f extends uniquely to a M -adically continuous function $f: \hat{A}^n \rightarrow \hat{A}$.*

3. A few technicalities

This section contains lemmata needed for the investigation of the spectrum of $\text{Int}_D(A)$ and, for commutative A , of $\text{Int}_D^n(A)$. From now on, all statements about $\text{Int}_D^n(A)$ are subject to the convention: if A is non-commutative, assume $n \leq 1$.

3.1 Lemma. *Let D be a domain and P a finitely generated prime ideal of height 1. For every non-zero $p \in P$ there exist $m \in \mathbb{N}$ and $s \in D \setminus P$ such that $sP^m \subseteq pD$.*

Proof. Let $p \in P$. In the localization D_P , P_P is the radical of (q) for every non-zero $q \in P_P$. Therefore, since P (and hence P_P) is finitely generated, there exists $m \in \mathbb{N}$ with $P_P^m \subseteq pD_P$ and in particular $P^m \subseteq pD_P$.

The ideal P^m is also finitely generated, by p_1, \dots, p_k , say. Let $a_i \in D_P$ with $p_i = pa_i$. By considering the fractions $a_i = r_i/s_i$ (with $r_i \in D$ and $s_i \in D \setminus P$), and setting $s = s_1 \cdot \dots \cdot s_k$, we see that $sP^m \subseteq pD$ as desired. \square

3.2 Definition. If $S \subseteq B^n$ and $T \subseteq B$, let

$$\text{Int}_D^n(S, T) = \{f \in K[x_1, \dots, x_n] \mid f(S) \subseteq T\}.$$

3.3 Lemma. *Let D be a domain and P a finitely generated prime ideal of height 1. Then every prime ideal Q of $\text{Int}_D^n(A)$ with $Q \cap D = P$ contains $\text{Int}_D^n(A, PA)$.*

Proof. Let $f \in \text{Int}_D^n(A, PA)$. By dint of Lemma 3.1, there are $m \in \mathbb{N}$, $p \in P$ and $s \in D \setminus P$ such that $sP^m \subseteq pD$. Then $sf^m \in \text{Int}_D^n(A, pA) = p \text{Int}_D^n(A) \subseteq Q$. As Q is prime and $s \notin Q$, we conclude that $f \in Q$. \square

3.4 Lemma. *Let A be a D -algebra that is finitely generated as a D -module, M a maximal ideal of finite index in D and \hat{A} the M -adic completion of A . For all $a \in \hat{A}^n$, the ideal $(M\hat{A})_a = \{f \in \text{Int}_D^n(A) \mid f(a) \in M\hat{A}\}$ is of finite index in $\text{Int}_D^n(A)$.*

Proof. Since A is a finitely generated D -module, \hat{A} is a finitely generated \hat{D} -module. As \hat{M} is of finite index in \hat{D} , $\hat{A}/M\hat{A}$ is finite. Let $\text{Int}_D^n(A)(a)$ denote the image of a under $\text{Int}_D^n(A)$. Then $\text{Int}_D^n(A)(a)/(M\hat{A} \cap \text{Int}_D^n(A)(a))$, as a subring of $\hat{A}/M\hat{A}$, is finite.

Let b_1, \dots, b_m be a system of representatives of $\text{Int}_D^n(A)(a)$ modulo $M\hat{A} \cap \text{Int}_D^n(A)(a)$, and for $1 \leq i \leq m$ let $f_i \in \text{Int}_D^n(A)$ with $f_i(a) = b_i$. Then for every $f \in \text{Int}_D^n(A)$, exactly one of the differences $f - f_i$ is in $(M\hat{A})_a$, which means that $\{f_1, \dots, f_m\}$ is a complete system of residues of $\text{Int}_D^n(A)(a)$ modulo $(M\hat{A})_a$. We have shown $[\text{Int}_D^n(A) : (M\hat{A})_a] = [\text{Int}_D^n(A)(a) : M\hat{A} \cap \text{Int}_D^n(A)(a)] \leq [\hat{A} : M\hat{A}] \quad \square$

4. Primes lying over a height one maximal ideal of finite index.

In this section we determine the prime ideals of $\text{Int}_D(A)$ (and, for commutative A , of $\text{Int}_D^n(A)$) lying over a height one prime ideal of finite index of D . Prime ideals lying over a prime of infinite index in D will be characterized in the next section.

4.1 General hypotheses in this section.

- (i) D is a domain and A a torsion-free D -algebra, finitely generated as a D -module;
- (ii) M is a finitely generated maximal ideal of height 1 and finite index in D ;
- (iii) $MA_M \cap A = MA$. (Note that $MA_M \cap A = MA$ is satisfied in two important cases: if A is a free D -module, and if $D \subseteq A$ is an extension of Dedekind rings.)

We denote the M -adic completions of D and A by \hat{D} and \hat{A} . Since M is finitely generated, M -adic and \hat{M} -adic topologies coincide on \hat{D} and on \hat{A} .

4.2 Lemma. *The hypotheses of 4.1 imply*

- (iv) $M\hat{A} \cap A = MA$.
- (v) \hat{D} and \hat{A} are compact.

Proof. (iv) Whenever M is a finitely generated maximal ideal of height 1 in a domain D and A a finitely generated D -module, the equality $M\hat{A} \cap A = MA_M \cap A$ holds, by [1, Chapter III, §2.12, Prop. 16] combined with [1, §3.5, Cor. 1 of Prop. 9].

(v) The ring \hat{D} is compact because M is of finite index and finitely generated, which implies that all powers of M are of finite index. \hat{A} then is compact because it is finitely generated as a \hat{D} -module. \square

4.3 Notation. Recall our convention that we only allow $n > 1$ in $\text{Int}_D^n(A)$ if A is commutative; for non-commutative A , $n = 1$ is assumed.

The image of $a \in \hat{A}$ under $\text{Int}_D^n(A)$ and $\text{Int}_D(A)$ we denote as follows:

$$\text{Int}_D^n(A)(a) = \{f(a) \mid f \in \text{Int}_D^n(A)\} \quad \text{and} \quad \text{Int}_D(A)(a) = \{f(a) \mid f \in \text{Int}_D(A)\}.$$

If M is a maximal ideal of D and $a \in \hat{A}^n$ let

$$(M\hat{A})_a = \{f \in \text{Int}_D^n(A) \mid f(a) \in M\hat{A}\}.$$

If P is an ideal of a commutative ring between $\text{Int}_D^n(a)$ and \hat{A} , let

$$P_a = \{f \in \text{Int}_D^n(A) \mid f(a) \in P\}.$$

4.4 Lemma. *Under the hypotheses of 4.1, let Q be a prime ideal of $\text{Int}_D^n(A)$ lying over M . Then there exists $a \in \hat{A}$ such that*

$$(M\hat{A})_a \subseteq Q.$$

In particular, Q is of finite index.

Proof. Suppose Q does not contain any $(M\hat{A})_a$. Then for every $a \in \hat{A}^n$ there exists $f \in (M\hat{A})_a \setminus Q$. By Theorem 2.3, f is M -adically continuous, so there exists an M -adic neighborhood U of a , such that $f(U) \subseteq M\hat{A}$. By compactness of \hat{A}^n , there exist finitely many a_i such that the corresponding neighborhoods U_i cover \hat{A}^n . Let g be the product of the polynomials $f_i \in (M\hat{A})_{a_i} \setminus Q$ with $f_i(U_i) \subseteq M\hat{A}$. For all $a \in A$, $g(a) \in M\hat{A} \cap A = MA_M \cap A = MA$ (by Lemma 4.2). Since Q is prime, $g \notin Q$, and yet $g \in \text{Int}_D^n(A, MA)$, a contradiction to Lemma 3.3. We have shown that Q contains some $(M\hat{A})_a$, which is of finite index by Lemma 3.4. \square

In the special case $A = D$, the preceding lemma already concludes the characterization of primes of $\text{Int}_D^n(D)$ lying above a maximal ideal M of finite index in D (a result of Chabert [6]), because then $(M\hat{A})_a$ is $(M\hat{D})_a = \{f \in \text{Int}_D^n(D) \mid f(a) \in \hat{M}\}$, a prime ideal of finite index, and hence maximal. Chabert, however, showed the other inclusion, $Q \subseteq (M\hat{A})_a$, after first showing independently that Q must be maximal [3, Prop. V.2.2].

4.5 Lemma. *Under the hypotheses of 4.1, let Q be a prime ideal of $\text{Int}_D^n(A)$ lying over M . For every $a \in \hat{A}$ such that $(M\hat{A})_a \subseteq Q$, there exists a maximal ideal P of $\text{Int}_D^n(A)(a)$ such that $Q = P_a$.*

Proof. Since $\hat{A}/M\hat{A}$ is a finite ring, $\text{Int}_D^n(A)(a)/(\text{Int}_D^n(A)(a) \cap M\hat{A})$ is a finite commutative ring. Let P_1, \dots, P_k be the maximal ideals of $\text{Int}_D^n(A)(a)$ containing $\text{Int}_D^n(A)(a) \cap M\hat{A}$.

Suppose Q is not contained in any $(P_i)_a$, for $1 \leq i \leq k$. Then, by prime avoidance, $Q(a) = \{f(a) \mid f \in Q\}$ is not contained in $\bigcup_{i=1}^k P_i$. Let $f \in Q$ such that $f(a)$ is not in any P_i . Then the residue class of $f(a)$ is a unit in $\text{Int}_D^n(A)(a)/(\text{Int}_D^n(A)(a) \cap M\hat{A})$.

Replacing f by a suitable power of f (using the fact that the group of units of $\text{Int}_D^n(A)(a)/(\text{Int}_D^n(A)(a) \cap M\hat{A})$ is finite) we see that there exists $f \in Q$ with $f(a) \equiv 1 \pmod{M\hat{A}}$. It follows that $1 - f \in (M\hat{A})_a \subseteq Q$ and therefore $1 \in Q$, a contradiction. \square

4.6 Theorem. *Let D be a domain, A a torsion-free D -algebra finitely generated as a D -module, M a finitely generated maximal ideal of D of finite index and height one, such that $MA_M \cap A = MA$.*

The prime ideals of $\text{Int}_D^n(A)$ lying over M are precisely the ideals of the form

$$P_a = \{f \in \text{Int}_D^n(A) \mid f(a) \in P\},$$

where $a \in \hat{A}$ (the M -adic completion of A), and P is a maximal ideal of $\text{Int}_D^n(A)(a)$ (the image of a under $\text{Int}_D^n(A)$) with $P \cap D = M$. In particular, all primes of $\text{Int}_D^n(A)$ lying over M are of finite index.

Proof. There exist primes of $\text{Int}_D^n(A)$ lying over M , because $(M\hat{A})_a$ with $a \in \hat{A}$ is a proper ideal of $\text{Int}_D^n(A)$ containing M .

If Q is a prime ideal of $\text{Int}_D^n(A)$ lying over M , then Lemma 4.4 shows that there exists an element $a \in \hat{A}$ such that $(M\hat{A})_a$ is contained in Q , and that Q is of finite index. It then follows from Lemma 4.5 that $Q = P_a$ for some maximal ideal P of $\text{Int}_D^n(A)(a)$ satisfying $M \subseteq \text{Int}_D^n(A)(a) \cap M\hat{A} \subseteq P$, and hence $P \cap D = M$.

Conversely, if P is a maximal ideal of $\text{Int}_D^n(A)(a)$, then $\text{Int}_D^n(A)/P_a$ is isomorphic to $\text{Int}_D^n(A)(a)/P$. Therefore P_a is a maximal ideal of $\text{Int}_D^n(A)(a)$. \square

It may happen that we do not know the exact image of $a \in \hat{A}$ under $\text{Int}_D^n(A)$, but do know a commutative ring R_a between $\text{Int}_D^n(A)(a)$ and \hat{A} . In this case we should remember that $R_a/(R_a \cap M\hat{A})$ is a subring of the finite ring $(\hat{A}/M\hat{A})$, and that therefore $\text{Int}_D^n(A)(a)/(\text{Int}_D^n(A)(a) \cap M\hat{A}) \subseteq (R_a/R_a \cap M\hat{A})$ is an extension

of finite commutative rings. Since extensions of finite commutative rings satisfy “lying over”, every prime ideal of $\text{Int}_D^n(A)(a)$ comes from a prime ideal of R_a , and we conclude:

4.7 Corollary. *Under the hypotheses of Theorem 4.6, suppose we have, for every $a \in \hat{A}$, a commutative ring R_a with $\text{Int}_D^n(A)(a) \subseteq R_a \subseteq \hat{A}$.*

Then the prime ideals of $\text{Int}_D^n(A)$ are precisely the ideals of the form

$$P_a = \{f \in \text{Int}_D^n(A) \mid f(a) \in P\},$$

where $a \in \hat{A}$ and P is a maximal ideal of R_a lying over M .

If A is a commutative D -algebra, we can take $R_a = \hat{A}$ in Corollary 4.7 for all $a \in \hat{A}$, and we get the following simpler characterization of the primes of $\text{Int}_D^n(A)$ lying over M :

4.8 Theorem. *Let D be a domain, A a commutative torsion-free D -algebra finitely generated as a D -module, M a finitely generated maximal ideal of D of finite index and height one, such that $MA_M \cap A = MA$.*

Then every prime ideal of $\text{Int}_D^n(A)$ lying over M is of the form

$$P_a = \{f \in \text{Int}_D^n(A) \mid f(a) \in P\},$$

for some $a \in \hat{A}$ (the M -adic completion of A) and P a maximal ideal of \hat{A} lying over M . In particular, every prime of $\text{Int}_D^n(A)$ lying over M is of finite index.

5. Primes lying over prime ideals of infinite index

5.1 Lemma. *Let A be a torsion-free D -algebra with $K \cap A = D$. Let P be a prime ideal of infinite index in D and $n \in \mathbb{N}$. Then $\text{Int}_D^n(A) \subseteq D_P[x_1, \dots, x_n]$.*

Proof. More generally, we show that for any prime ideal P , a polynomial $f \in \text{Int}_D^n(A)$ of degree less than $[D : P]$ in every individual variable is in $D_P[x_1, \dots, x_n]$. We use induction on n . The case $n = 0$ is trivial: $\text{Int}_D^0(D) = K \cap A = D \subseteq D_P$.

For $n > 0$ consider f as a polynomial in x_n with coefficients in $K[x_1, \dots, x_{n-1}]$. Let $s \leq [D : P]$ such that f is of degree strictly less than s in each x_j .

Choose $d_1, \dots, d_s \in D \subseteq A$ pairwise incongruent mod P . For every i , the value of f at d_i (substituted for x_n) is a polynomial in $\text{Int}_D^{n-1}(A)$ of degree less than

s in each variable. Therefore $f(x_1, \dots, x_{n-1}, d_i) \in D_P[x_1, \dots, x_{n-1}]$, by induction hypothesis.

Let $g \in K(x_1, \dots, x_{n-1})[x_n]$ be the Lagrange interpolation polynomial with $g(d_i) = f(x_1, \dots, x_{n-1}, d_i)$ ($1 \leq i \leq s$); then $g \in D_P[x_1, \dots, x_{n-1}][x_n]$. Since a polynomial (with coefficients in a domain) of degree less than s is determined by its values at s different arguments, we must have $f = g \in D_P[x_1, \dots, x_{n-1}][x_n]$. \square

5.2 Corollary. *Let A be a torsion-free D -algebra with $K \cap A = D$. If all maximal ideals of D are of infinite index, then $\text{Int}_D^n(A) = D[x_1, \dots, x_n]$.*

Alternatively, we could have deduced the previous lemma from the corresponding fact for the ring of integer-valued polynomials over D [3, Prop. I.3.4, XI.1.10], since after all $\text{Int}_D^n(A) \subseteq \text{Int}(D^n) = \{f \in K[x_1, \dots, x_n] \mid f(D^n) \subseteq D\}$.

5.3 Lemma. *Let A be a torsion-free D -algebra with $K \cap A = D$. Let P be a prime ideal of infinite index in D and $n \in \mathbb{N}$. Then the prime ideals of $\text{Int}_D^n(A)$ lying over P are precisely those of the form $Q \cap \text{Int}_D^n(A)$, where Q is a prime ideal of $D_P[x_1, \dots, x_n]$ containing $PD_P[x_1, \dots, x_n]$.*

Proof. As $D[x_1, \dots, x_n] \subseteq \text{Int}_D^n(A) \subseteq D_P[x_1, \dots, x_n] = D[x_1, \dots, x_n]_{(D \setminus P)}$, we have

$$D_P[x_1, \dots, x_n] = \text{Int}_D^n(A)_{(D \setminus P)}$$

and therefore a bijective correspondence (given by lying over) exists between prime ideals of $\text{Int}_D^n(A)$ whose intersection with D is contained in P and prime ideals of $D_P[x_1, \dots, x_n]$. \square

5.4 Theorem. *Let D be a Noetherian one-dimensional domain with finite residue fields and A a torsion-free D algebra, finitely generated as a D -module, such that for every maximal ideal M , $MA_M \cap D = M$. If A is commutative, let $n \in \mathbb{N}$, for non-commutative A restrict to $n = 1$. Then $\text{Int}_D^n(A)$ is $(n + 1)$ -dimensional.*

Proof. By Lemma 5.3, the prime ideals of $\text{Int}_D^n(A)$ lying over (0) all come from prime ideals of $K[x_1, \dots, x_n]$. The primes of $\text{Int}_D^n(A)$ lying over a maximal ideal M are all maximal and hence mutually incomparable. So $\dim(\text{Int}_D^n(A)) \leq n + 1$. If M is a maximal ideal of D and $d = (d_1, \dots, d_n) \in D^n$, let \mathcal{Q}_k be the ideal of $K[x_1, \dots, x_n]$ generated by $(x_1 - d_1), \dots, (x_k - d_k)$. Then a chain of primes of length $n + 1$ of $\text{Int}_D^n(A)$ is given by $Q_0 = (0)$, $Q_k = \mathcal{Q}_k \cap \text{Int}_D^n(A)$, for $k = 1, \dots, n$ and $Q_{n+1} = P_d = \{f \in \text{Int}_D^n(A) \mid f(d_1, \dots, d_n) \in P\}$, where P is a maximal ideal of the image of d under $\text{Int}_D^n(A)$. \square

5.5 Remark. If D is a Noetherian domain of characteristic 0, finitely generated as a \mathbb{Z} -algebra, such as, for instance, the ring of integers \mathcal{O}_K in a number field, then no maximal ideal of $\text{Int}_D^n(A)$ lies over (0) of D . This holds for $A = D$ by [3, Prop. XI.3.4.], and carries over to $\text{Int}_D^n(A)$, since $\text{Int}_D^n(A) \subseteq \text{Int}(D^n)$. Every prime ideal P of $\text{Int}_D^n(A)$ coming from a prime ideal of $K[x_1, \dots, x_n]$ is contained in a maximal ideal Q of $\text{Int}(D^n)$ lying over a maximal ideal M of D , and $Q \cap \text{Int}_D^n(A)$ then properly contains P .

5.6 Remark. Even if there are no maximal ideals lying over (0) , maximal chains of primes of $\text{Int}_D^n(A)$ are not necessarily of length $n + 1$. For instance, a maximal ideal of $\text{Int}_D^n(A)$ may well have height 1 if it is of the form $(M\hat{A})_a$ for $a = (a_1, \dots, a_n) \in \hat{A}^n$ with a_1, \dots, a_n algebraically independent over K .

6. Integer-valued polynomials on matrix algebras

Theorem 4.6 characterizes the spectrum of the ring $\text{Int}_D(A)$, provided we know the images of elements of M -adic completions of A under $\text{Int}_D(A)$. We will now determine these images in the case $A = M_n(D)$. Note that all the technical hypotheses in this section are certainly satisfied if $D = \mathcal{O}_K$ is the ring of integers in a number field.

6.1 Fact. [10, Lemma 2.2] *Let D be a domain and $f(x) = g(x)/d$ with $g \in D[x]$, $d \in D \setminus \{0\}$. Then $f \in \text{Int}_D(M_n(D))$ if and only if g is divisible modulo $dD[x]$ by all monic polynomials in $D[x]$ of degree n .*

6.2 Proposition*. *Let D be a domain such that the intersection of the maximal ideals of D of finite index is (0) , and $f(x) = g(x)/d$ with $g \in D[x]$, $d \in D \setminus \{0\}$. Then $f \in \text{Int}_D(M_n(D))$ if and only if g is divisible modulo $dD[x]$ by all monic irreducible polynomials in $D[x]$ of degree n .*

Proof. In view of Fact 6.1, it suffices to show for every $d \in D \setminus \{0\}$ and $h \in D[x]$ monic of degree n , that there exists $k \in D[x]$ monic of degree n , irreducible in $D[x]$ and congruent to $h \pmod{dD[x]}$. We may choose a maximal ideal P of finite index with $d \notin P$, and use Chinese remainder theorem on the coefficients of h to find $k \in D[x]$, monic of degree n , congruent to $h \pmod{dD[x]}$ and irreducible in $(D/P)[x]$. \square

We are now able to identify a polynomially dense subset of $M_n(D)$ consisting of companion matrices. They are often easier to work with than general matrices, because their characteristic polynomial is also their minimal polynomial.

6.3 Theorem*. *Let \mathcal{C}_n be the set of companion matrices of monic polynomials of degree n in $D[x]$ and $\mathcal{I}_n \subseteq \mathcal{C}_n$ the subset of companion matrices of irreducible polynomials. If D is any domain,*

$$\text{Int}_D(M_n(D)) = \text{Int}_D(\mathcal{C}_n, M_n(D)).$$

If D is a domain such that the intersection of the maximal ideals of finite index is (0) , such as, for instance, a Dedekind domain with infinitely many maximal ideals of finite index, then

$$\text{Int}_D(M_n(D)) = \text{Int}_D(\mathcal{I}_n, M_n(D)).$$

Proof. Let $f \in \text{Int}_D(\mathcal{C}_n, M_n(D))$, $f(x) = g(x)/d$ with $g \in D[x]$, $d \in D$. Since g maps every $C \in \mathcal{C}_n$ to $M_n(dD)$, g is divisible mod $dD[x]$ by every monic polynomial in $D[x]$ of degree n . (This is so because f is still the minimal polynomial of its companion matrix when everything is viewed in D/dD .) By Fact 6.1, $f \in \text{Int}_D(M_n(D))$. This shows $\text{Int}_D(\mathcal{C}_n, M_n(D)) \subseteq \text{Int}_D(M_n(D))$. The reverse inclusion is trivial. The argument for \mathcal{I}_n is similar, using Prop. 6.2. \square

6.4 Theorem. *Let D be a domain and $C \in M_n(D)$. Let*

$$\text{Int}(A)(C) = \{f(C) \mid f \in \text{Int}_D(M_n(D))\} \quad \text{and} \quad D[C] = \{f(C) \mid f \in D[x]\}.$$

Then $\text{Int}(A)(C) = D[C]$.

Proof. Consider $f \in \text{Int}_D(M_n(D))$; $f(x) = g(x)/d$ with $g \in D[x]$ and $d \in D \setminus \{0\}$. We know that g is divisible modulo $dD[x]$ by every monic polynomial in $D[x]$ of degree n . Dividing g by χ_C , the characteristic polynomial of C , we get

$$g(x) = q(x)\chi_C(x) + dr(x)$$

with $q, r \in D[x]$ and we see that that $f(C) = r(C)$. Thus $\text{Int}(A)(C) \subseteq D[C]$. The reverse inclusion is clear, since $D[x] \subseteq \text{Int}_D(M_n(D))$. \square

6.5 Definition. A local domain is called *analytically irreducible* if its completion is also a domain.

6.6 Lemma. *Let M be a maximal ideal of finite index in a domain D . Then the following are equivalent*

- (1) $\bigcap_{n=1}^{\infty} M^n = (0)$ and D_M is analytically irreducible
- (2) for every non-zero $d \in D$, cancellation of d is uniformly M -adically continuous.

Proof. (1 \Rightarrow 2) We have to show: for every non-zero $d \in D$, for every $m \in \mathbb{N}$ there exists $k \in \mathbb{N}$ such that for all $c \in D$: $dc \in M^k$ implies $c \in M^m$. Indirectly, suppose there exists $d \in D \setminus \{0\}$ and $m \in \mathbb{N}$, such that for every $k \in \mathbb{N}$ there is some $c_k \in D$ with $dc_k \in M^k$ and $c_k \notin M^m$. Since \hat{D} is compact and satisfies first countability axiom, (c_k) has a convergent subsequence. Its limit $c \in \hat{D}$ satisfies $c \notin M^m$, and hence $c \neq 0$, and also for all k , $dc \in M^k$, which implies $dc = 0$. We have shown the existence of zero-divisors in \hat{D} .

(2 \Rightarrow 1) is easy. \square

6.7 Theorem. *Let D be a domain, M a maximal ideal of finite index of D such that $\bigcap_{n=1}^{\infty} M^n = (0)$ and D_M is analytically irreducible. Let \hat{D} be the M -adic completion of D , $C \in M_n(\hat{D})$, and $\text{Int}_D(M_n(D))(C)$ the image of C under $\text{Int}_D(M_n(D))$. Then*

$$\text{Int}_D(M_n(D))(C) \subseteq \hat{D}[C].$$

Proof. Let $f \in \text{Int}_D(M_n(D))$, $f(x) = g(x)/d$ with $g \in D[x]$, $d \in D$. For every $m \in \mathbb{N}$ let $k_m \in \mathbb{N}$ such that for all $c \in D$, $cd \in M^{k_m}$ implies $c \in M^m$. Let $E_1 = (e_{ij}^{(1)})$ and $E_2 = (e_{ij}^{(2)})$ be matrices in $M_n(D)$ with characteristic polynomials χ_1 and χ_2 . Then $g(x) = q_i(x)\chi_i(x) + dr_i(x)$ with $q_i, r_i \in D[x]$ for $i = 1, 2$. If $e_{ij}^{(1)} \equiv e_{ij}^{(2)} \pmod{M^{k_m}}$, then $dr_1 \equiv dr_2 \pmod{M^{k_m}D[x]}$, and therefore $r_1 \equiv r_2 \pmod{M^mD[x]}$. We can therefore M -adically approximate C by matrices C_i with $f(C_i) = s_i(C_i)$ with $s_i \in D[x]$, $\deg s_i < n$, such that the s_i converge towards a polynomial $s \in \hat{D}[x]$ with $\deg s < n$ and $f(C) = s(C)$. \square

6.8 Corollary. *Let D be a Dedekind domain, M a maximal ideal of finite index, \hat{D} the M -adic completion of D , and $C \in M_n(\hat{D})$. Then*

$$\text{Int}_D(M_n(D))(C) \subseteq \hat{D}[C].$$

7. Integer-valued polynomials with matrix coefficients

While we have been investigating the ring $\text{Int}_D(M_n(D))$ of polynomials in $K[x]$ mapping matrices in $M_n(D)$ to matrices in $M_n(D)$, Werner [13] has been studying the set, let's call it $\text{Int}_D[M_n(D)]$ with square brackets, of polynomials with coefficients in the non-commutative ring $M_n(K)$ mapping matrices in $M_n(D)$ to matrices in $M_n(D)$. Without substitution homomorphism, it is not a priori clear that this set is closed under multiplication, but Werner [13] has shown that it is, and so $\text{Int}_D[M_n(D)]$ is actually a ring between $(M_n(D))[x]$ and $(M_n(K))[x]$.

Also in [13], Werner proves that every ideal of $\text{Int}_D[M_n(D)]$ can be generated by elements of $K[x]$. Using the idea of his proof, one can show more: $\text{Int}_D[M_n(D)]$ is isomorphic to the algebra of $n \times n$ matrices over $\text{Int}_D(M_n(D))$. Since every prime ideal of a matrix ring is just the set of matrices with entries in a prime ideal of the ring, we get a description of the spectrum of $\text{Int}_D[M_n(D)]$ as a byproduct of our description of the spectrum of $\text{Int}_D(M_n(D))$ in the previous section. We recall the definition of prime ideal for non-commutative rings:

7.1 Definition. We call a two-sided ideal $P \neq R$ of a (not necessarily commutative) ring with identity R a prime ideal, if, for all ideals A, B of R ,

$$AB \subseteq P \implies A \subseteq P \text{ or } B \subseteq P,$$

or equivalently, if, for all $a, b \in R$

$$aRb \subseteq P \implies a \in P \text{ or } b \in P.$$

For commutative R this is equivalent to the (in general stronger) condition: for all $a, b \in R$,

$$ab \in P \implies a \in P \text{ or } b \in P.$$

7.2 Theorem. Let D be a domain with quotient field K , and

$$\begin{aligned} \text{Int}_D(M_n(D)) &= \{f \in K[x] \mid \forall C \in M_n(D) : f(C) \in M_n(D)\} \\ \text{Int}_D[M_n(D)] &= \{f \in (M_n(K))[x] \mid \forall C \in M_n(D) : f(C) \in M_n(D)\}. \end{aligned}$$

We identify $\text{Int}_D[M_n(D)] \subseteq (M_n(K))[x]$ with its isomorphic image in $M_n(K[x])$ under

$$\varphi: (M_n(K))[x] \rightarrow M_n(K[x]), \quad \sum_k (a_{ij}^{(k)})_{1 \leq i, j \leq n} x^k \mapsto \left(\sum_k a_{ij}^{(k)} x^k \right)_{1 \leq i, j \leq n}$$

Then $\text{Int}_D[M_n(D)] = M_n(\text{Int}_D(M_n(D)))$.

Proof. Note that $K[x]$ is embedded in $M_n(K[x])$ as the subring of scalar matrices $g(x)I_n$, and in $M_n(K)[x]$ as the subring of polynomials $g(x)$ whose coefficients are scalar matrices rI_n , with $r \in K$. Clearly, $\text{Int}_D[M_n(D)] \cap K[x] = \text{Int}_D(M_n(D))$.

Let $C = (c_{ij}(x)) \in \text{Int}_D[M_n(D)] \subseteq M_n(K[x])$. Let e_{ij} be the matrix in $M_n(D)$ with 1 in position (i, j) and zeros elsewhere; then $e_{ij}Ce_{kl}$ has $c_{jk}(x)$ in position (i, l) and zeros elsewhere. Also, $e_{ij}Ce_{kl} \in \text{Int}_D[M_n(D)]$, since $\text{Int}_D[M_n(D)]$ is a ring containing $M_n(D)$. So $\sum_{i=1}^n e_{ij}Ce_{ki} = c_{jk}(x)I_n \in \text{Int}_D[M_n(D)]$. Therefore $c_{jk}(x) \in K[x] \cap \text{Int}_D[M_n(D)] = \text{Int}_D(M_n(D))$ for all (j, k) , and hence $\text{Int}_D[M_n(D)] \subseteq M_n(\text{Int}_D(M_n(D)))$.

Conversely, if $f \in \text{Int}_D(M_n(D))$ then $f(x)I_n \in \text{Int}_D[M_n(D)]$. Therefore, $e_{ik}f(x)I_n e_{kl}$, the matrix containing $f(x)$ in position (i, l) and zeros elsewhere, is in $\text{Int}_D[M_n(D)]$, for arbitrary (i, l) . By summing matrices of this kind we see that $M_n(\text{Int}_D(M_n(D))) \subseteq \text{Int}_D[M_n(D)]$. \square

For any ring R with identity the ideals of R are in bijective correspondence with the ideals of $M_n(R)$ by $I \mapsto M_n(I)$, and restriction to prime ideals gives a bijection between the spectrum of R and the spectrum of $M_n(R)$. So we conclude:

7.3 Corollary. *Let $\text{Int}_D(M_n(D))$ and $\text{Int}_D[M_n(D)]$ as in the preceding theorem. Under the identification of $\text{Int}_D[M_n(D)]$ with its isomorphic image in $M_n(K[x])$,*

- (1) *The two-sided ideals of $\text{Int}_D[M_n(D)]$ are precisely the sets of the form $M_n(I)$, where I is an ideal of $\text{Int}_D(M_n(D))$.*
- (2) *The two-sided prime ideals of $\text{Int}_D[M_n(D)]$ are precisely the sets of the form $M_n(P)$, where P is a prime ideal of $\text{Int}_D(M_n(D))$.*

Acknowledgments. The author wishes to thank J.-L. Chabert for helpful hints, in particular Lemma 4.2 (iv), and P.-J. Cahen for improving Lemma 3.1.

References

- [1] N. BOURBAKI, *Commutative Algebra, Chapters 1–7*, Springer, 1989.
- [2] J. BOYNTON AND L. KLINGLER, *The n -generator property in rings of integer-valued polynomials determined by finite sets*, Arch. Math. (Basel) 86 (2006), 36–42.
- [3] P.-J. CAHEN AND J.-L. CHABERT, *Integer-valued polynomials*, vol. 48 of Mathematical Surveys and Monographs, Amer. Math. Soc., 1997.
- [4] P.-J. CAHEN, J.-L. CHABERT, AND S. FRISCH, *Interpolation domains*, J. Algebra 225 (2000), 794–803.

- [5] P.-J. CAHEN, J.-L. CHABERT, AND K. A. LOPER, *High dimension Prüfer domains of integer-valued polynomials*, J. Korean Math. Soc. 38 (2001), 915–935.
- [6] J.-L. CHABERT, *Les idéaux premiers de l’anneau des polynômes à valeurs entières*, J. Reine Angew. Math. 293/294 (1977), 275–283.
- [7] Q. CHANG, *A sort of polynomial identities of $M_n(F)$ with $\text{char } F \neq 0$* , Chinese Ann. Math. Ser. B 9 (1988), 161–166.
- [8] S. FRISCH, *Interpolation by integer-valued polynomials*, J. Algebra 211 (1999), 562–577.
- [9] S. FRISCH, *Nullstellensatz and Skolem properties for integer-valued polynomials*, J. Reine Angew. Math. 536 (2001), 31–42.
- [10] S. FRISCH, *Polynomial separation of points in algebras*, in Arithmetical Properties of Commutative Rings and Monoids (Chapel Hill Conf. 2003), S. Chapman, ed., vol. 241 of Lecture Notes in Pure and Applied Mathematics, Chapman & Hall/CRC, 2005, 253–259.
- [11] K. A. LOPER, *A classification of all D such that $\text{Int}(D)$ is a Prüfer domain*, Proc. Amer. Math. Soc. 126 (1998), 657–660.
- [12] K. A. LOPER AND N. J. WERNER, *Generalized rings of integer-valued polynomials*, J. Number Theory 132 (2012), 2481–2490.
- [13] N. J. WERNER, *Integer-valued polynomials over matrix rings*, Comm. Algebra 40 (2012), 4717 – 4726.
- [14] A. E. ZALESSKIĬ, *A symmetric analogue of the Amitsur-Levitzki theorem*, Vestsi Akad. Navuk BSSR Ser. Fiz.-Mat. Navuk (1985), 108–110, 128.

Institut für Mathematik A
 Technische Universität Graz
 Steyrergasse 30
 A-8010 Graz, Austria
 frisch@TUGraz.at

Corrigendum for “INTEGER-VALUED POLYNOMIALS ON ALGEBRAS
[J. Algebra 373 (2013) 414-425]”, appeared in J. Algebra 412 (2014) p 282

Sophie Frisch frisch@TU Graz.at

In this paper in J. Algebra 373 (2013) 414-425, in Prop. 6.2 and Thm. 6.3,
instead of “a domain with zero Jacobson radical” we need the stronger assumption
“a domain such that the intersection of all maximal ideals of finite index is zero”.