Actes des rencontres du CIRM 2 (2010) no 2, pp 27-32; http://acirm.cedram.org/acirm-bin/browse

INTEGER-VALUED POLYNOMIALS ON ALGEBRAS A SURVEY

SOPHIE FRISCH

Abstract. We compare several different concepts of integer-valued polynomials on algebras and collect the few results and many open questions to be found in the literature. (2000 Math. Subj. Classification: Primary 13F20; Secondary 16S50, 13B25, 13J10, 11C08, 11C20)

1. Introduction

Let D be a domain with quotient field K. The popular ring of integer-valued polynomials $\mathrm{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\}$ has been generalized to polynomials acting on non-commutative algebras in different ways by different authors. Some consider polynomials with coefficients in K that map a given D-algebra to itself. For instance, Loper [5] and the present author [2, 3] have investigated polynomials with rational coefficients mapping $n \times n$ integer matrices to integer matrices.

Others consider polynomials with coefficients in a non-commutative K-algebra that map a given D-subalgebra to itself. For instance, Werner [7] has investigated polynomials with coefficients in the rational quaternions mapping integer quaternions to integer quaternions; Werner [6] and the present author [2] have looked at polynomials with coefficients in $M_n(K)$ mapping matrices in $M_n(D)$ to matrices in $M_n(D)$.

Before we give a precise definition of two types of rings of integer-valued polynomials on algebras, a few examples (in one variable). For lack of a better idea, we write the first kind of integer-valued polynomial rings, those with coefficients in K, with parentheses: $\mathrm{Int}_{\mathrm{D}}(A)$, and the second kind, those with coefficients in a K-algebra, with square brackets: $\mathrm{Int}_{\mathrm{D}}[A]$. Throughout this paper, D is an integral domain, not a field, with quotient field K.

Example 1.1. For fixed $n \in \mathbb{N}$, consider

$$\mathrm{Int}_{\mathrm{D}}(\mathrm{M}_n(D)) = \{f \in K[x] \mid \forall C \in \mathrm{M}_n(D) :\ f(C) \in \mathrm{M}_n(D)\}$$
$$\mathrm{Int}_{\mathrm{D}}[\mathrm{M}_n(D)] = \{f \in (\mathrm{M}_n(K))[x] \mid \forall C \in \mathrm{M}_n(D) :\ f(C) \in \mathrm{M}_n(D)\}.$$

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

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

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

$$\begin{aligned} \mathrm{Int}_{\mathrm{D}}(D(G)) &= \{f \in K[x] \mid \forall z \in D(G) : \ f(z) \in D(G)\} \\ \mathrm{Int}_{\mathrm{D}}[D(G)] &= \{f \in K(G)[x] \mid \forall z \in D(G) : \ f(z) \in D(G)\} \end{aligned}$$

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

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

Convention 1.5. Let D be a domain and not a field, K the quotient field of D, and A a torsion-free D-algebra that is finitely generated as a D-module.

Since A is faithful, we have an isomorphic copy of D embedded in A (by $d \mapsto d1_A$). Let $B = K \otimes_D A$ (canonically isomorphic to the ring of fractions $A_{D\setminus\{0\}}$). Then the natural homomorphisms $\iota_K : K \to K \otimes_D A$, $k \mapsto k \otimes 1_A$ and $\iota_A : A \to K \otimes_D A$, $a \mapsto 1_K \otimes a$ allow us to evaluate in B polynomials with coefficients in K or B at arguments in A, and we define:

$$\mathrm{Int}_{\mathrm{D}}(A) = \{f \in K[x] \mid \forall a \in A : \ f(a) \in A\}$$
$$\mathrm{Int}_{\mathrm{D}}[A] = \{f \in (K \otimes_D A)[x] \mid \forall a \in A : \ f(a) \in A\}$$

Note that ι_K and ι_A are injective whenever A is a torsion-free D-module. To exclude unwanted cases such as $A = K$ we require $K \cap A = D$ (or, more precisely, $\iota_K(K) \cap \iota_A(A) = \iota_A(D)$).

Note that $K \cap A = D$ implies

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

With the conventions above, $\mathrm{Int}_{\mathrm{D}}(A)$ is easily seen to be a ring. In particular, $\mathrm{Int}_D(A)$ is closed with respect to multiplication, because $(fg)(a) = f(a)g(a)$ for all $a \in A$ and $f, g \in K[x]$. By the same token, $\mathrm{Int}_D[A]$ is a ring for commutative A. The argument involving subsitution homomorphism works only in the commutative case, however. For non-commutative A, multiplicative closure of $\mathrm{Int}_D[A]$ is not evident. We will look into this in the next section.

2. Non-commutatve coefficient rings

Theorem 2.1 (Werner [6])**.** *If A is finitely generated by units as a D-algebra, then $\mathrm{Int}_{\mathrm{D}}[A]$ is closed under multiplication and hence a ring.*

Proof. Let $f(x) = \sum_k \beta_k x^k$ and $g(x)$ be in $\mathrm{Int_D}[A]$ and $\alpha \in A$. To show $(fg)(\alpha) \in A$, we first check the special case where $g = u$, a unit in A:

$$(fu)(\alpha) = \sum_k \beta_k u \alpha^k = \sum_k \beta_k (u\alpha u^{-1})^k u = f(u\alpha u^{-1})u \in A.$$

Now for general $f, g \in \mathrm{Int_D}[A]$:

$$(fg)(\alpha) = \sum_{m,l} \beta_m \gamma_l \alpha^{m+l} = \sum_m \beta_m (\sum_l \gamma_l \alpha^l)\alpha^m = \sum_m \beta_m g(\alpha)\alpha^m.$$

Expressing $g(\alpha)$ as a D-linear combination of units $u_1, \ldots, u_n$ of A,

$$g(\alpha) = d_1 u_1 + \ldots + d_n u_n,$$

yields

$$(fg)(\alpha) = \sum_m \beta_m (\sum_{j=1}^n d_j u_j)\alpha^m = \sum_{j=1}^n d_j \sum_m \beta_m u_j \alpha^m = \sum_{j=1}^n d_j (fu_j)(\alpha).$$

Since $d_j \in D$ and each $(fu_j)(\alpha)$ is in A, it follows that $(fg)(\alpha)$ is in A. □

Remark 2.2. In all three non-commutative examples in the introduction, A is generated as a D-module by units, and $\mathrm{Int_D}[A]$ is a therefore a ring. In example 1.1, for instance, the free D-module $M_n(D)$ of dimension n^2 has the following basis (suggested by L. Vaserstein) consisting of matrices of determinant 1: let $E_{i,j}(\lambda)$ for $i \neq j$ denote the elementary matrix with ones on the diagonal, λ in position (i, j) and zeros elsewhere. As basis, take the $n^2 - n$ elementary matrices $E_{i,j}(1)$ for $i \neq j$, together with the n products of two elementary matrices $E_{i,i+1}(1)E_{i+1,i}(-1)$ for $1 \leq i \leq n$ (with indices mod n, i.e., $n + 1 = 1$).

One of the rings of the form $\mathrm{Int_D}[A]$ for non-commutative A that have been examined in some detail is $\mathrm{Int}_{\mathbb{Z}}[L]$, the ring of polynomials with coefficients in the rational quaternions mapping integer quaternions to integer quaternions. Werner [7] has shown $\mathrm{Int_D}[A]$ to be non-Noetherian, and has exhibited some prime ideals.

In his forthcoming paper [6], Werner explores $\mathrm{Int_D}[M_n(D)]$, and shows that every ideal of this ring is generated as a left $M_n(D)$-module by elements of $K[x]$. Using ideas from [6], one can show more, however: the ring $\mathrm{Int_D}[\mathrm{M}_n(D)]$ of polynomials with coefficients in $M_n(K)$ that map every matrix in $M_n(D)$ to a matrix in $M_n(D)$ is isomorphic to the ring of $n \times n$ matrices over the ring $\mathrm{Int_D}(\mathrm{M}_n(D))$ of polynomials in $K[x]$ that map every matrix in $M_n(D)$ to a matrix in $M_n(D)$.

Theorem 2.3 ([2]). *Let*

$$\mathrm{Int_D}(\mathrm{M}_n(D)) = \{f \in K[x] \mid \forall C \in M_n(D):\ f(C) \in M_n(D)\},$$
$$\mathrm{Int_D}[\mathrm{M}_n(D)] = \{f \in (M_n(K))[x] \mid \forall C \in M_n(D):\ f(C) \in M_n(D)\}.$$

We identify $\mathrm{Int_D}[\mathrm{M}_n(D)]$ *with its isomorphic image under the natural ring isomorphism*

$$\varphi\colon (M_n(K))[x] \to M_n(K[x]), \quad \sum_k (a_{ij}^{(k)})_{1\le i,j\le n}\, x^k \mapsto \left(\sum_k a_{ij}^{(k)} x^k\right)_{1\le i,j\le n}.$$

Then

$$\mathrm{Int_D}[\mathrm{M}_n(D)] = M_n(\mathrm{Int_D}(\mathrm{M}_n(D))).$$

Corollary 2.4. *Under the identification of* $\mathrm{Int_D}[M_n(D)]$ *with its isomorphic image in* $M_n(K[x])$*, the ideals of* $\mathrm{Int_D}[M_n(D)]$ *are precisely the sets of the form* $M_n(I)$*, where* I *is an ideal of* $\mathrm{Int_D}(M_n(D))$*. Prime ideals of* $\mathrm{Int_D}[M_n(D)]$ *correspond to prime ideals of* $\mathrm{Int_D}(M_n(D))$ *and vice versa.*

Our definition of prime ideal for a possibly non-commutative ring is: a two-sided ideal $P \ne R$, such that for any two-sided ideals A, B of R, $AB \subseteq R$ implies $A \subseteq P$ or $B \subseteq P$.

It might be interesting to generalize Theorem 2.3 to other rings of integer-valued polynomials on a D-algebra A with coefficients in a non-commutative K-algebra B. Given a matrix representation $B \subseteq M_n(K)$, we can identify the ring $\mathrm{Int_D}[A] \subseteq B[x]$ of polynomials with coefficents in B, integer-valued on A, with its image in $M_n(K[x])$ under the isomorphism of $(M_n(K))[x]$ with $M_n(K[x])$.

- Starting with a matrix representation $B \subseteq M_n(K)$, is the isomorphic image of $\mathrm{Int_D}[A] \subseteq (M_n(K))[x]$ embedded in $M_n(K[x])$ a matrix algebra over a ring of integer-valued polynomials with coefficents in K?

3. The Spectrum

We now return to commuting coefficents and describe the spectrum of $\mathrm{Int_D}(A)$. If A is a commutative D-algebra, we also consider polynomials is several variables and define

$$\mathrm{Int_D^n} = \{f \in K[x_1, \ldots, x_n] \mid \forall a \in A^n : f(a) \in A\}.$$

Prime ideals lying over a prime P of infinite index of D are easy to describe: they all come from prime ideals of $D_P[x]$ (or $D_P[x_1, \ldots, x_n]$, for $\mathrm{Int_D^n}(A)$), since $\mathrm{Int_D}(A) \subseteq \mathrm{Int}(D) \subseteq D_P[x]$ (and $\mathrm{Int_D^n}(A) \subseteq \mathrm{Int}(D^n) \subseteq D_P[x_1, \ldots, x_n]$) whenever $[D : P] = \infty$ (cf. [1]).

Concerning primes lying over a maximal ideal M of finite index of D, they have been characterized for one-dimensional Noetherian D in [2]. For commutative A, they look just like the maximal ideals of $\mathrm{Int}(D)$.

Note that the somewhat technical condition $MA_M \cap A = MA$ is satisfied in two natural cases, firstly, if A is a free D-module, and secondly, if $D \subseteq A$ is an extension of Dedekind rings.

Theorem 3.1 ([2]). *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 $MA_M \cap A = MA$, and $n \in \mathbb{N}$.*

Then every prime ideal of $\mathrm{Int}^{\mathrm{n}}_{\mathrm{D}}(A)$ lying over M is maximal, and of the form

$$P_a = \{f \in \mathrm{Int}^{\mathrm{n}}_{\mathrm{D}}(A) \mid f(a) \in P\},$$

for some $a \in \hat{A}$ (the M-adic completion of A) and P a maximal ideal of $\hat{A}$ with $P \cap D = M$.

In the case of a non-commutative D-algebra A, the images of elements $a \in \hat{A}$ under $\mathrm{Int}_{\mathrm{D}}(A)$ play a rôle in the description of the maximal ideals lying above M. If the exact image $\mathrm{Int}_{\mathrm{D}}(A)(a)$ is not known, it can be replaced by a commutative ring R_a between $\mathrm{Int}_{\mathrm{D}}(A)(a)$ and $\hat{A}$.

Theorem 3.2 ([2]). *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 $\mathrm{Int}_{\mathrm{D}}(A)$ lying over M are precisely the ideals of the form

$$P_a = \{f \in \mathrm{Int}_{\mathrm{D}}(A) \mid f(a) \in P\},$$

where $a \in \hat{A}$ (the M-adic completion of A), and P is a maximal ideal of $\mathrm{Int}_{\mathrm{D}}(A)(a)$ (the image of a under $\mathrm{Int}^{\mathrm{n}}_{\mathrm{D}}(A)$) with $P \cap D = M$.

We can replace $\mathrm{Int}_{\mathrm{D}}(A)(a)$ by a commutative ring R_a with $\mathrm{Int}_{\mathrm{D}}(A)(a) \subseteq R_a \subseteq \hat{A}$ for the simple reason that every extension of finite commutative rings, in particular the ring extension $\mathrm{Int}_{\mathrm{D}}(A)(a)/(\mathrm{Int}_{\mathrm{D}}(A)(a) \cap M\hat{A}) \subseteq R_a/(R_a \cap M\hat{A})$ satisfies "lying over".

Corollary 3.3. *Under the hypotheses of of Theorem 3.2, suppose we are given, for every $a \in \hat{A}$, a commutative ring R_a with $\mathrm{Int}_{\mathrm{D}}(A)(a) \subseteq R_a \subseteq \hat{A}$.*

Then the prime ideals of $\mathrm{Int}_{\mathrm{D}}(A)$ are precisely the ideals of the form

$$P_a = \{f \in \mathrm{Int}_{\mathrm{D}}(A) \mid f(a) \in P\},$$

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

For $A = M_n(D)$, and $a \in A$, the image of a under $\mathrm{Int}(A)(a)$ is just $D[a]$, and for a general $a \in \hat{A}$, the image of a under $\mathrm{Int}(A)(a)$ is contained in $\hat{D}[a]$ (cf. [2]), so that we may take $R_a = \hat{D}[a]$ in Corollary 3.3. For other algebras, the question is open:

- is there a simple description of the image of an element $a \in \hat{A}$ under $\mathrm{Int_D}(A)$?

Another property of the ring of integer-valued polynomials on matrices is waiting for generalization. If D is a domain with zero Jabobson radical, such as, for instance, a Dedekind ring with infinitely many maximal ideals, then the subset $\mathcal{C}$ of $M_n(D)$ consisting of the companion matrices of all monic irreducible polynomials in D is a polynomially dense subset of $M_n(D)$, i.e., every polynomial $f \in K[x]$ with $f(C) \in M_n(D)$ for every $C \in \mathcal{C}$ is in $\mathrm{Int_D}(M_n(D))$. This prompts the question, for a general D-algebra A,

- does A have a polynomially dense subset of elements with irreducible minimal polynomial in $K[x]$?

4. A non-triviality criterion

For rings of integer valued polynomials with coefficients in a field, of the type

$$\mathrm{Int_D}(A) = \{f \in K[x] \mid f(A) \subseteq A\},$$

or, for commutative A,

$$\mathrm{Int}^{\mathrm{n}}_{\mathrm{D}}(A) = \{f \in K[x_1, \ldots, x_n] \mid \forall a_1, \ldots, a_n \in A: \; f(a_1, \ldots, a_n) \in A\},$$

we have the inclusions

$$D[x] \subseteq \mathrm{Int_D}(A) \subseteq \mathrm{Int}(D) \subseteq K[x],$$

and similarly for several variables. As before, D is a domain with quotient field K, A a torsion-free D-algebra finitely generated as a D-module, and evaluation of polynomials is performed in $B = K \otimes_D A$. As noted in the introduction, we also require (of the homomorphic images in B) that $K \cap A = D$.

$\mathrm{Int_D}(A)$ is considered trivial if $\mathrm{Int_D}(A) = D[x]$. We will see that the non-triviality criterion for $\mathrm{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\}$ for Noetherian D ([1] Thm. I.3.14) carries over to $\mathrm{Int_D}(A)$.

Lemma 4.1. *Let A be a torsion-free D-algebra that is finitely generated as a D-module, and let $n \in \mathbb{N}$. If there exists a proper ideal of D of the form $I = (b :_D c)$ (with $b, c \in D$) of finite index, then* $\mathrm{Int}^{\mathrm{n}}_{\mathrm{D}}(A) \neq D[x_1, \ldots, x_n]$.

Proof. Say A is generated by d elements as a D-module. Then every element of A is integral of degree at most d over D. Given $I = (b :_D c) \neq D$ of finite index, let $f \in D[x]$ be a monic polynomial that is divisible modulo $I[x]$ by every monic polynomial of degree at most d. Then for every $a \in A$, $f(a) \in IA$, and hence

$\frac{c}{b}f(a) \in A$. If follows that $\frac{c}{b}f(x)$ is in $\mathrm{Int_D}(A)$ (as well as in $\mathrm{Int^n_D}(A)$ for all $n \geq 1$), but not in $D[x]$, since its leading coefficient $\frac{c}{b}$ is not in D. $\square$

Lemma 4.2. *If, for some $n \in \mathbb{N}$, $\mathrm{Int^n_D}(A) \neq D[x_1, \ldots, x_n]$ then there exists a proper ideal of D of the form $I = (b :_D c)$ (with $b, c \in D$) such that every prime ideal P of D containing I is of finite index.*

Proof. Let $b, c \in D$ such that $k = \frac{c}{b} \notin D$ occurs as a coefficient of a polynomial in $\mathrm{Int^n_D}(A)$. If P is a prime ideal of infinite index in D, then $\mathrm{Int^n_D}(A) \subseteq D_P[x_1, \ldots, x_n]$; so there exists some $s \in D \setminus P$ with $sk \in D$, i.e., with $s \in (b :_D c)$. This means that $(b :_D c)$ is not contained in any prime ideal of infinite index. $\square$

It is easy to see that, for arbitrary fixed $b \in D$, an ideal that is maximal among proper ideals of the form $(b : d)$ (with $d \in D$) is prime. In a Noetherian domain D therefore, every proper ideal $I = (b : c)$ is contained in a prime ideal $P = (b : d)$. This shows that for a Noetherian domain D and a D-algebra A whose elements are integral of bounded degree over D, the necessary and the sufficient condition for $\mathrm{Int_D}(A) \neq D[x]$ (in 4.1 and 4.2, respectively) are each equivalent to: D has a prime ideal of finite index of the form $P = (b : d)$.

If, given an ideal I of D, we call a prime ideal of the form $(I :_D d)$ (with $d \in D$) an *associated prime ideal* of I then our criterion for non-triviality of $\mathrm{Int^n_D}(A)$ in the Noetherian case becomes:

Theorem 4.3. *Let D be a Noetherian domain and A a torsion-free D-algebra that is finitely generated as a D-module and let $n \in \mathbb{N}$. Then $\mathrm{Int^n_D}(A) \neq D[x_1, \ldots, x_n]$ if and only if D has a prime ideal of finite index that is an associated prime of a principal ideal of D.*

A different question of non-triviality is, whether $\mathrm{Int_D}(A)$ is properly contained in $\mathrm{Int}(D)$. (Recall that $\mathrm{Int_D}(A) \subseteq \mathrm{Int}(D)$ follows from our convention $K \cap A = D$.) Let K be a number field and $\mathcal{O}_K$ its ring of algebraic integers. It has been shown by Halter-Koch and Narkiewicz [4] that $\mathrm{Int}_{\mathbb{Z}}(\mathcal{O}_K)$ is always properly contained in $\mathrm{Int}(\mathbb{Z})$. For general D and A it is an open question,

- under what hypotheses is $\mathrm{Int_D}(A) \subsetneq \mathrm{Int}(D)$?

5. Prüfer or not Prüfer

For rings of integer-valued polynomials on algebras of the type

$$\mathrm{Int}_{\mathbb{Z}}(A) = \{f \in \mathbb{Q}[x] \mid f(A) \subseteq A\},$$

for a $\mathbb{Z}$-algebra A, the big question is, what are criteria for $\mathrm{Int}_{\mathbb{Z}}(A)$ to be Prüfer, or just to be integrally closed?

In some interesting special cases Loper [5] has the answer:

Theorem 5.1 (Loper [5]).

(1) *Let $\mathcal{O}_K$ be the ring of algebraic integers in the number field K. Then* $\mathrm{Int}_{\mathbb{Z}}(\mathcal{O}_K)$ *is Prüfer.*
(2) *Let $M_2(\mathbb{Z})$ be the ring of 2×2 integer matrices, then* $\mathrm{Int}_{\mathbb{Z}}(M_2(\mathbb{Z}))$ *is not Prüfer.*
(3) *Let L be the ring of integer (Lipschitz) quaternions. Then* $\mathrm{Int}_{\mathbb{Z}}(L)$ *is not Prüfer.*

In cases 2 and 3, Loper shows that the ring in question is not Prüfer by exhibiting an overring that is not integrally closed. For any non-commutative $\mathbb{Z}$-algebra A, such as $A = M_n(\mathbb{Z})$ or $A = L$, this prompts the following questions:

- Is $\mathrm{Int}_{\mathbb{Z}}(A)$ integrally closed?
- What is its integral closure?
- Is the integral closure Prüfer?

References

[1] P.-J. Cahen and J.-L. Chabert, *Integer-valued polynomials*, vol. 48 of Mathematical Surveys and Monographs, Amer. Math. Soc., 1997.
[2] S. Frisch, *Integer-valued polynomials on algebras*, preprint.
[3] S. Frisch, *Polynomial separation of points in algebras*, in Arithmetical Properties of Commutative Rings and Monoids (Chapel Hill Conf. 2003), S. Chapman, ed., Dekker, 2005, 249–254.
[4] F. Halter-Koch and W. Narkiewicz, *Commutative rings and binomial coefficients*, Mh. Math 114 (1992), 107–110.
[5] K. A. Loper, *A generalization of integer-valued polynomial rings*, preprint.
[6] N. J. Werner, *Integer-valued polynomials over matrix rings*, preprint.
[7] N. J. Werner, *Integer-valued polynomials over quaternion rings*, J. Algebra (2010), 1754–1769.

Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria
E-mail address: `frisch@TUGraz.at`