in: S. Chapman (ed.), Arithmetical Properties of Commutative Rings and Monoids (Chapel Hill Conf. 2003), Lect. Notes in Pure and Appl. Math. vol. 241, Chapman&Hall CRC 2005, pp 253–259.

Polynomial Separation of Points in Algebras

SOPHIE FRISCH Institut für Mathematik, Technische Universität Graz, A-8010 Graz, Austria email: frisch@blah.math.tu-graz.ac.at

ABSTRACT. We show that for a wide variety of domains, including all Dedekind rings with finite residue fields, it is possible to separate any two algebraic elements a, b of an algebra over the quotient field by integer-valued polynomials (i.e. to map a and b to 0 and 1, respectively, with a polynomial in $K[x]$ that maps every element of D to an element of D), provided only that the minimal polynomials of a and b in $K[x]$ are co-prime (which is obviously necessary).

In contrast to this, it is impossible to separate $a, b \in D$ by a $n \times n$-integer-matrix-valued polynomial (a polynomial in $K[x]$ that maps every $n \times n$ matrix over D to a matrix with entries in D), except in the trivial case where $a-b$ is a unit of D. (This is despite the fact that the ring of $n \times n$-integer-matrix-valued polynomials for any fixed n is non-trivial whenever the ring of integer-valued polynomials is non-trivial.) 2000 Math. Subj. Classification: Primary 13F20; Secondary 13B25, 11C08, 15A36, 16B99.

1 INTRODUCTION

Definition 1.1. If D is a domain with quotient field K, the ring of integer-valued polynomials of D is

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

Rings of integer-valued polynomials have proved remarkably well suited for interpolation purposes.

Definition 1.2. A domain D is called *interpolation domain*, if for all $n \in \mathbb{N}$, for all $a_1, \ldots, a_n \in D$ (distinct) and all $b_1, \ldots, b_n \in D$ there exists $f \in \mathrm{Int}(D)$ with $f(a_i) = b_i$ for $1 \leq i \leq n$.

Interpolation domains have been classified both among Noetherian domains and among Prüfer domains in [3] (see also Corollary 2.4). In particular, every Dedekind domain all of whose residue fields are finite is an interpolation domain.

Equivalent to being an interpolation domain is the following point separation property: for any a, $b \in D$ with $a \neq b$ there exists a polynomial $f \in \mathrm{Int}(D)$ with $f(a) = 0$ and $f(b) = 1$.

In this note we explore two possible avenues for extending this point separation property to D-algebras and K-algebras. If D is a domain for which separation of points in D by polynomials in $\mathrm{Int}(D)$ is possible, we ask ourselves

(1) Can elements in an arbitrary K-algebra (for instance the ring of $n \times n$ matrices with entries in K) be separated by polynomials in $\mathrm{Int}(D)$?

(2) Can elements of D be separated by polynomials in $K[x]$ that map a given D-algebra (for instance the ring of $n \times n$ matrices with entries in D) to itself?

It turns out that the answer to (1) is yes, within reason (the minimal polynomials of the elements to be separated have to be co-prime in $K[x]$); but (2) may fail spectacularly for D-algebras with zero-divisors. We will show that it is impossible to separate points in D by polynomials in $K[x]$ that map $M_n(D)$ (the D-algebra of $n \times n$ matrices with entries in D) to itself, except in trivial cases.

2 SEPARATION OF POINTS IN AN ALGEBRA

The basic connections between separation of points, co-maximality of null-ideals, and interpolation hold in great generality, so we state them for functions - even though we are only concerned with polynomials in this paper.

Throughout this paper, every ring or algebra (commutative or not) is assumed to have an identity element (and every ring homomorphism to satisfy $\varphi(1) = 1$). D and K stand for a domain and its quotient field; R denotes a ring (possibly non-commutative, possibly with zero-divisors).

Notation and Conventions. Let R be a ring and S a set. We say that a ring $\mathcal{F}$ is a *ring of functions* from S to R if $\mathcal{F}$ comes equipped with a ring homomorphism $\psi\colon \mathcal{F} \to R^S (= \prod_{s\in S} R)$ assigning to each element $f \in \mathcal{F}$ a function (which we also call f, by abuse of notation).

If $(\mathcal{F}, \psi)$ is a ring of functions from S to R and $s \in S$, we call

$$N_{\mathcal{F}}(s) = \{f \in \mathcal{F} \mid f(s) = 0\}$$

the *null-ideal* of s in $\mathcal{F}$.

We say that we can *separate* points in S by functions from $\mathcal{F}$ if for all $s, t \in S$ with $s \neq t$ there exists an $f \in \mathcal{F}$ with $f(s) = 0$ and $f(t) = 1$.

We say that we can *interpolate* arbitrary functions from S to R by functions in $\mathcal{F}$ if for all $n \in \mathbb{N}$, for all $s_1, \ldots, s_n \in S$ (distinct) and all $r_1, \ldots, r_n \in R$ there exists some $f \in \mathcal{F}$ with $f(s_i) = r_i$ for $1 \leq i \leq n$.

Lemma 2.1. *Let $(\mathcal{F}, \psi)$ be a ring of functions from S to R.*

(i) *For s, $t \in S$, there exists an $f \in \mathcal{F}$ with $f(s) = 0$ and $f(t) = 1$ if and only if*

$$N_{\mathcal{F}}(s) + N_{\mathcal{F}}(t) = \mathcal{F}.$$

(ii) *To be able to interpolate arbitrary functions from S to R by functions in $\mathcal{F}$ it is necessary and, if $\mathcal{F}$ is an R-algebra and ψ an R-algebra homomorphism, also sufficient, to be able to separate points in S by functions in $\mathcal{F}$.*

Proof. (i) is easy; and, ad (ii), separation of points is clearly necessary for interpolation. If $\mathcal{F}$ is an R-algebra then, given $s_1, \ldots, s_n \in S$ which we can mutually separate, we have functions $f_{ij} \in \mathcal{F}$ with $f_{ij}(s_i) = 1$ and $f_{ij}(s_j) = 0$, which we multiply to get a Lagrange interpolation function $f_i \in F$ with $f_i(s_i) = 1$ and $f_i(s_j) = 0$ for $j \neq i$. Then we can use R-linear combinations of the f_i to interpolate. $\square$

Proposition 2.2. *Let D be a domain with quotient field K. D is an interpolation domain if and only if it has the following property: whenever a_1, a_2 are algebraic elements of a K-algebra A, whose minimal polynomials in $K[x]$ are co-prime, there exists a polynomial $p \in \mathrm{Int}(D)$ with $p(a_1) = 0$ and $p(a_2) = 1$.*

Proof. Assume D is an interpolation domain. Given a_1, a_2 with co-prime minimal polynomials f_1, $f_2 \in K[x]$, let c_1, c_2 be non-zero elements of D such that $c_i f_i = g_i \in D[x]$. There exist polynomials $p_i \in D[x]$ and a non-zero constant $d \in D$ such that

$$g_1(x)p_1(x) + g_2(x)p_2(x) = d.$$

Let $h(x) \in \mathrm{Int}(D)$ with $h(0) = 1$ and $h(d) = 0$, and set

$$p(x) = h(g_2(x)p_2(x)) = h(d - g_1(x)p_1(x)),$$

then $p(a_1) = 0$ and $p(a_2) = 1$.

Conversely, the point separation property for K-algebras specialized to $A = K$ implies separation of points in D by polynomials in $\mathrm{Int}(D)$ which by Lemma 2.1 (ii) implies interpolation of arbitrary functions from D to D by polynomials in $\mathrm{Int}(D)$. $\square$

If D is a Dedekind domain with finite residue fields, the construction of the point separating integer-valued polynomial h in the preceding proof can be made fairly explicit, cf. [4].

Corollary 2.3. *A domain D with quotient field K is an interpolation domain if and only if for any f_1, $f_2 \in K[x]$ with*

$$K[x]f_1(x) + K[x]f_2(x) = K[x]$$

it follows that

$$(K[x]f_1(x) \cap \mathrm{Int}(D)) + (K[x]f_2(x) \cap \mathrm{Int}(D)) = \mathrm{Int}(D).$$

Proof. In view of Lemma 2.1 and Proposition 2.2, all that remains to show is that every two non-constant monic polynomials in $K[x]$ occur as minimal polynomials of two elements of the same K-algebra. This can be seen by looking at the companion matrices of the polynomials in question, bringing the smaller matrix up to the size of the larger matrix by padding with zeros at the right and bottom. $\square$

Recalling the characterization of interpolation domains among Noetherian domains from [3] (Theorem 2.4.), we obtain:

Corollary 2.4. *Let D be a Noetherian domain with quotient field K. Then the following are equivalent:*
(1) D is an interpolation domain

(2) *whenever a_1, a_2 are algebraic elements of a K-algebra A whose minimal polynomials in $K[x]$ are co-prime, there exists a polynomial $p \in \mathrm{Int}(D)$ with $p(a_1) = 0$ and $p(a_2) = 1$*

(3) *whenever I, J are ideals of $K[x]$ with $I + J = K[x]$ then*

$$(I \cap \mathrm{Int}(D)) + (J \cap \mathrm{Int}(D)) = \mathrm{Int}(D)$$

(4) *D is one-dimensional with finite residue fields and locally unibranched (the last condition meaning that the integral closure of every localization at a prime ideal is again local).*

3 INTEGER-MATRIX-VALUED POLYNOMIALS

Definition 3.1. We denote by $\mathrm{Mint}_n(D)$ the ring of polynomials in $K[x]$ that map $n \times n$ matrices with entries in D to matrices with entries in D:

$$\mathrm{Mint}_n(D) = \{f \in K[x] \mid \forall A \in M_n(D) : \ f(A) \in M_n(D)\}.$$

Clearly,

$$K[x] \supseteq \mathrm{Int}(D) \supseteq \mathrm{Mint}_2(D) \supseteq \mathrm{Mint}_3(D) \supseteq \ldots \supseteq D[x],$$

and, as Lemma 3.4 below shows, $\bigcap_{n=1}^{\infty} \mathrm{Mint}_n(D) = D[x]$.

Example 3.2. One may ask if $\mathrm{Mint}_n(D)$ is not often trivial, in the sense of $\mathrm{Mint}_n(D) = D[x]$. The answer is, for Noetherian D at least: not more often than $\mathrm{Int}(D)$ is trivial. (This can be shown by combining the proof of Theorem I.3.14 of [2] with Lemma 3.4 below). It follows immediately from Lemma 3.4 that $\mathrm{Mint}_n(D) \neq D[x]$ (for any $n \geq 1$) whenever D has a proper principal ideal of finite index. For example,

$$\frac{x^6 + x^5 + x^3 + x^2}{2} \quad \text{is in} \quad \mathrm{Mint}_2(\mathbb{Z}) \setminus \mathrm{Mint}_3(\mathbb{Z}).$$

(The residue class of $x^6 + x^5 + x^3 + x^2$ in $\mathbb{Z}_2[x]$ is the least common multiple of all monic polynomials in $\mathbb{Z}_2[x]$ of degree 2.)

When investigating $\mathrm{Mint}_n(D)$, it is useful to know in what cases the null ideal of a matrix $A \in M_n(R)$ in the polynomial ring $R[x]$ is principal, not just for $R = D$, but also for residue class rings $R = D/I$. If D is a domain then $N_{D[x]}(A) = \{f \in D[x] \mid f(A) = 0\}$ is principal for every matrix $A \in M_n(D)$ if and only if D is integrally closed [5]. But even for the most mundane commutative ring R we know that the null ideals in $R[x]$ of some matrices are principal. (Thanks to Gabriel Picavet for pointing this out):

Lemma 3.3. *Let R be a commutative ring, $f \in R[x]$ a monic polynomial and $A \in M_n(R)$ the companion matrix of f. Then $N_{R[x]}(A) = f(x)R[x]$.*

Proof. By a theorem of McCoy ([1], Theorem 7.31) the null ideal in $R[x]$ of a matrix $A \in M_n(R)$ is $(F_n :_{R[x]} F_{n-1})$, where F_k denotes the ideal generated in $R[x]$ by the $k \times k$ minors of $xI_n - A$ (I_n the $n \times n$ identity matrix). For any A, $F_n = c_A(x)R[x]$ (c_A the characteristic polynomial of A); and if A is the companion matrix of a polynomial, then one of the $(n-1) \times (n-1)$ minors of $xI_n - A$ is 1, such that in this case the null ideal of A is $c_A(x)R[x] = f(x)R[x]$. □

Lemma 3.4. *Let D be a domain and $f(x) = g(x)/c$, $g \in D[x]$, $c \in D \setminus \{0\}$. Then $f \in \mathrm{Mint}_n(D)$ if and only if g is divisible modulo $cD[x]$ by all monic polynomials in $D[x]$ of degree n.*

Proof. Suppose $f \in \mathrm{Mint}_n(D)$. Let $\bar{g}$ denote the residue class of g in $(D/cD)[x]$. Then $\bar{g}$ maps every matrix in $M_n(D/cD)$ to the zero-matrix. In particular, this holds for all companion matrices of monic polynomials of degree n. Therfore $\bar{g}$ is divisible in $(D/cD)[x]$ by all monic polynomials of degree n.

Conversely, this condition suffices for $f \in \mathrm{Mint}_n(D)$, because it means that g is divisible modulo $cD[x]$ by the characteristic polynomial of every matrix in $M_n(D)$, and therefore maps every matrix in $M_n(D)$ to a matrix in $M_n(cD)$. □

We are now ready to show that the rings $\mathrm{Mint}_n(D)$ are as unsuitable as can be for separation of points. For $n > 1$, $\mathrm{Mint}_n(D)$ cannot even separate elements $a, b \in D$, except in the trivial case when $a - b$ is a unit and they can be separated by the polynomial $(x - b)/(a - b) \in D[x]$.

Theorem 3.5. *Let D be a domain and $a, b \in D$. If there exists a polynomial $f \in \mathrm{Mint}_2(D)$ with $f(a) = 1$ and $f(b) = 0$ then $a - b$ is a unit of D.*

Proof. By linear substitution we can reduce to the case $a = 0$. Let $f \in \mathrm{Mint}_2(D)$ with $f(0) = 1$ and $f(b) = 0$. We write f as $f(x) = g(x)/c$ with $g \in D[x]$ and $c \neq 0$ in D. It follows that $c = g(0)$ and $g(x) = (x - b)h(x)$ with $h \in D[x]$.

By Lemma 3.4, g is divisible modulo $cD[x]$ by all monic polynomials in $D[x]$ of degree 2, in particular by $(x - b)x$.

In $(D/cD)[x]$ we have, for some $k \in (D/cD)[x]$,

$$(x - b)xk(x) = \bar{g}(x) = (x - b)\bar{h}(x)$$

and we can cancel $(x - b)$ which, being monic, is certainly not a zero-divisor in $(D/cD)[x]$. This shows that $\bar{h}$, the residue class of h in $(D/cD)[x]$, is divisible by x. Therefore, in $D[x]$, the constant coefficient of h is divisible by c, say $h(0) = dc$. Looking at the constant coefficient of g we have $c = g(0) = -bh(0) = -bdc$. Cancelling $c \neq 0$ proves $-b$ to be a unit of D. □

REFERENCES

[1] W. C. Brown, Matrices over Commutative Rings, vol. 169 of Pure and Applied Mathematics, Dekker, 1993.

[2] P.-J. Cahen and J.-L. Chabert, Integer-valued polynomials, vol. 48 of Mathematical Surveys and Monographs, Amer. Math. Soc., 1997.

[3] P.-J. Cahen, J.-L. Chabert, and S. Frisch, Interpolation domains, J. Algebra, 225 (2000), pp. 794–803.

[4] S. Frisch, Interpolation by integer-valued polynomials, J. Algebra, 211 (1999), pp. 562–577.

[5] ——, Integrally closed domains, minimal polynomials, and null ideals of matrices, Comm. Algebra, 32 (2004), pp. 2015–2017.

Corrigendum. After publication I discovered a slight mistake in the proof of Corollary 2.3. The corollary itself is correct. Here's how to fix the proof: Given two non-constant monic polynomials f and g in $K[x]$, we want a K-algebra A that has two elements a and b whose minimal polynomials are f and g. The matrices given in the paper won't work. What does work is: let C_f and C_g be the companion matrices of f and g, let $A = M_n(K)$, with $n = \operatorname{lcm}(\deg f, \deg g)$ and let a and b be block diagonal matrices, such that the blocks of a are all equal to C_f and the blocks of b are all equal to C_g.