ISRAEL JOURNAL OF MATHEMATICS, Vol. 31, Nos. 3-4, 1978

POLYNOMIALS OVER DIVISION RINGS

BY

S. A. AMITSUR AND LANCE W. SMALL[†]

ABSTRACT

Let D be a division ring with a center C, and $D[X_1,\cdots,X_N]$ the ring of polynomials in N commutative indeterminates over D. The maximum number N for which this ring of polynomials is primitive is equal to the maximal transcendence degree over C of the commutative subfields of the matrix rings $M_n(D)$, $n = 1,2,\cdots$. The ring of fractions of the Weyl algebras are examples where this number N is finite. A tool in the proof is a non-commutative version of one of the forms of the "Nullstellensatz", namely, simple $D[X_1,\cdots,X_m]$-modules are finite-dimensional D-spaces.

1. Introduction

Although there is a rich literature about polynomials in many (commuting) variables over commutative fields, and the polynomial ring in one variable over non-commutative division rings, there is relatively little known about the polynomial ring in several variables over a non-commutative division ring. In this paper we shall study two aspects of such polynomial rings.

First, we shall prove a "Nullstellensatz" for these rings. That is, if D is an arbitrary division ring then simple (one-sided) $D[X_1,\cdots,X_n]$-modules are finite-dimensional vector spaces over D. Here, $D[X_1,\cdots,X_n]$ is the polynomial ring in n commuting variables over D.

Second, we shall use this result to study the primitivity of these polynomial rings. It has been known for many years that if D is a division ring containing an element not algebraic over its center then $D[X_1]$ is primitive. Herstein, in conversation, asked whether the primivitivity of $D[X_1]$ "forced" the primitivity of the polynomial rings $D[X_1,\cdots,X_n]$. Using a criterion for primitivity following from the Nullstellensatz and results of Richard Resco [3], we shall construct division rings, $D^{(j)}$, j a positive integer, such that $D[X_1,\cdots,X_j]$ is primitive, but $D[X_1,\cdots,X_k]$ is not primitive for $k > j$.

[†] This paper was written while the authors were Fellows of the Institute for Advanced Studies, The Hebrew University of Jerusalem, Mount Scopus, Jerusalem, Israel.

Received May 12, 1978

Throughout this paper all rings will have unit elements, all modules will be left modules and all one-sided conditions will be on the left. If R is a ring then $C(R)$, or C when there is no ambiguity, will denote the center of R. $R[X_1,\cdots,X_n]$ will be the polynomial ring in n commuting indeterminates $X_1,\cdots,X_n$, over R. The left ideal generated by r R will be (r). Finally, if R is a ring, then $M_n(R)$ will denote the $n\times n$ matrices over R.

2. The Nullstellensatz

We prove

THEOREM 1. *If D is a division ring, then simple $D[X_1,\cdots,X_n]$-modules are finite-dimensional vector spaces over D.*

The proof of Theorem 1 is preceded by three lemmas.

LEMMA A. *Let D be a division ring and $0\neq p(t)\in D[t]$. Then there exist at most degree p different central irreducible polynomials $\phi(t)$ such that $g_\phi p\in\phi(t)D[t]$ and $g_\phi\notin\phi(t)D[t]$, for some g_ϕ.*

PROOF. If the lemma is incorrect, let p be of minimal degree for which there exist $\phi_1,\cdots,\phi_r$ irreducible central polynomials and $g_ip\in(\phi_i)$, $g_i\notin(\phi_i)$, $r>$ degree $p\geqq 1$. We divide the proof into two cases:

Case 1. There exist $y,x\in D[t]$ such that $py+\phi_rx=1$. Multiplying on the left by g_r, we obtain

$$g_r=g_rpy+\phi_rg_rx=\phi_r(h_ry+g_rx),$$

where $\phi_rh_r=g_rp\in(\phi_r)$. But $g_r\notin(\phi_r)$, and we have a contradiction.

Case 2. $fD[t]=pD[t]+\phi_rD[t]$, where $\deg f>0$. Write $p=fq$ where degree $q<$ degree $p<r$. Thus, degree $q<r-1$. On the other hand,

$$g_ip=(g_if)q\in(\phi_i)\qquad\text{for } i=1,2,\cdots,r-1$$

and, thus, by minimality of degree of p, we have for some j, $g_jf=\phi_ju$.

But there are central polynomials $a,b\in C[t]$ such that $\phi_ja+\phi_rb=1$, and by definition of f, $\phi_r=fe$ for some $e\in C[t]$. Hence

$$\phi_j\phi_r=g_jfe=(\phi_ju)e=\phi_j(ue)=\phi_jv.$$

On the other hand,

$$g_j=\phi_jag_j+\phi_rbg_j=\phi_jag_j+g_j\phi_rb=\phi_j(ag_j+vb)$$

because a, b and ϕ_r are central, thus contradicting $g_j\notin(\phi_j)$.

REMARK. The preceding lemma is readily extended to any finite set of polynomials $p_1, \cdots, p_s$. Namely, there exists at most a finite number of irreducible central polynomials ϕ for which there exists $g_{\phi i}$ satisfying $g_{\phi i}p_i \in (\phi)$, $g_{\phi i} \not\in (\phi)$. Hence, there exists a central irreducible φ such that $gp_i \in (\phi)$ for some i implies that $g \in (\varphi)$.

This follows from the fact that there are infinite (central) irreducible polynomials over any field $C \subseteq D$, of degree $\geqq 1$.

We need some preliminaries before the next lemma. Consider the monomial $X^{(\nu)} = X_1^{\nu_1} \cdots X_{n-1}^{\nu_{n-1}}$ in the first $n-1$ indeterminates of $R = D[X_1, \cdots, X_n]$. We order these monomials: $(\nu) > (\mu)$ if the first non-zero difference $\nu_1 - \mu_1, \cdots, \nu_{n-1} - \mu_{n-1}$ is positive. Thus, every polynomial in R can be written in the form

$$R[X_1, \cdots, X_{n-1}, X_n] = p_{(\nu)}[X_n]X^{(\nu)} + \sum_{(\mu)<(\nu)} P_{(n)}X^{(\mu)}.$$

We will call $p_{(\nu)}[X_n]$ the *highest coefficient* of p.

Now, let $0 \neq L$ be a left ideal in R. Denote by $L_{(\nu)}$ the set of all highest coefficients (and 0) of the polynomials in L of *degree* (ν). Clearly, $L_{(\nu)}$ is a left ideal in the ring $D[X_n]$. Futhermore, if, for (ν) and (μ), we have $\nu_i \geqq \mu_i$, for all i, then $L_{(\nu)} \supseteq L_{(\mu)}$. For if $p \in L$ is of degree (μ), then $X^{(\nu)-(\mu)}p \in L$ and is of degree (ν) with the same highest coefficient.

This last remark enables us to invoke a lemma of Diximier [2, p. 88, 2.6.2]: Let $\mathbf{N}$ be the non-negative integers and $\mathbf{N}^t$ the Cartesian product of $\mathbf{N}$ with itself t times. $\mathbf{N}^t$ can be partially ordered by $(n_1, \cdots, n_t) > (m_1, \cdots, m_t)$ if each $n_i > m_i$. Diximier's lemma asserts then that any infinite subset $y \in \mathbf{N}^t$ contains an infinite chain under the order.

We can now show

LEMMA B. *If L is left ideal of $D[X_1, \cdots X_n]$, then the set $\{L_{(\nu)}\}$, for all (ν), contains only a finite number of different left ideals.*

PROOF. If $\{L_{(\nu)}\}$ is infinite, consider the set $(\nu) \in \mathbf{N}^{(n-1)}$ of the infinite set $\{L_{(\nu)}\}$ of different ideal. We thus have an infinite subset of $\mathbf{N}^{(n-1)}$ and by Diximier's result we obtain an infinite set ascending chain under the order $>$. But this means we obtain an infinite (proper) ascending chain of left ideals in $D[X_n]$, which is impossible since $D[X_n]$ is a principal ideal ring.

Of independent interest is

LEMMA C. *If L is a maximal left ideal of $D[X_1, \cdots, X_n]$, then $L \cap D[X_k] \neq 0$ for all k.*

PROOF. We consider the case $k = n$. Let $L_{(\nu_{1\,1},\cdots,\nu_{1\,n-1})},\cdots,L_{(\nu_s\,1,\cdots,\nu_{sm-1})}$ be the finite set of non-zero different left ideals produced in Lemma B. Set $L_{(\nu_{i1},\cdots,\nu_{in-1})} = D[X_n]p_i[X_n]$. Choose a central, irreducible polynomial $\phi[X_n]$ in $D[X_n]$ which satisfies the condition: if $gp_i \in (\phi)$ then $g \in (\phi)$. The polynomial ϕ exists by the remark to Lemma A.

If $\phi[X_n] \in L$, then the lemma is proved; and if $\phi(X_n) \notin L$ then L maximal implies $D[X_1,\cdots,X_n]\phi(X_n) + L = D[X_1,\cdots,X_n]$. Thus

$$(*) \qquad 1 - Q(X_1,\cdots,X_n)\phi(X_n) \in L \qquad \text{for some } Q.$$

Pick Q of minimal degree $(r_1,\cdots,r_{n-1}) = (r)$ satisfying $(*)$. If $(r) = 0$, then the lemma is proved because $Q = Q(X_n)$ and so $1 - Q(X_n)\phi(X_n) \in L \cap D[X_n]$. If $(r) \neq 0$, $q_r\phi \in L_{(r)}$ where q_r is the highest coefficient of $Q(X_n,\cdots,X_n)$, but $L_{(r)} = L_{(\nu_{i\lambda})}$, for some i. Therefore $q_r\phi = gp_i$, hence $g = h(X_n)\phi(X_n)$ by the way ϕ was chosen. Now, there exists a $P(X_1,\cdots,X_n) \in L$ of degree (r) with highest coefficient p_i. Hence, $Q' = Q - hP$ will be a polynomial of degree less than (r). However $hP\phi = h\phi P \in L$, and in L we have

$$1 - Q\phi + hP\phi = 1 - (Q - hP)\phi = 1 - Q'\phi.$$

Hence Q' satisfies $(*)$ and is of lower degree than Q — a contradiction, and the lemma is proved.

We remark that we are unable to show that maximal left ideals in $D[X_i,\cdots,X_n]$ intersect $D[X_1,\cdots,X_k]$, $k < n$, in maximal or even semi-maximal left ideals.

The pieces are now available to prove our main result, Theorem 1.

PROOF OF THEOREM 1. If M is a simple $D[X_1,\cdots,X_n]$-module then $M \simeq D[X_1,\cdots,X_n]/L$, where L is a maximal left ideal. By Lemma C, $L \cap D[X_i] \neq 0$, for all i. Let $p_i(X_i) \in L \cap D[X_i]$ and degree $p_i(X_i) = n_i$. Then M is generated as a vector space over D by all monomials $X_1^{m_1},\cdots,X_n^{m_n}$, $m_i < n_i$, for all i, because the X_i commute.

3. Applications to primitivity

We begin this section by recalling a well-known result: If A is a central simple C-algebra and B is a C-algebra, then the two-sided ideals of $A \otimes_C B$ are precisely $A \otimes_C I$, where I is an ideal of B. Hence, if B is a prime ring, then $A \otimes_C B$ is also a prime ring.

The following proposition generalizes a basic tool in the study of finite-dimensional central simple algebras.

PROPOSITION. *If A is a central simple C-algebra, M an A-module of finite length and $B \subseteq \mathrm{End}_A M$ is a prime C-algebra, then $A \otimes_C B^{\mathrm{op}}$ is a primitive ring.*

PROOF. Since M is a faithful A-module and of finite length, we note that M is also a faithful left $A \otimes_C B^{\mathrm{op}}$-module of finite length. The last fact is trivial and proof of the first is as follows: Let $\mathrm{Ann}(M)$, as an $A \otimes_C B^{\mathrm{op}}$-module, be K. Then $K = A \otimes I^{\mathrm{op}}$, I an ideal in B. Thus, by the usual action, we have $AMI = 0$ which forces $MI = 0$ — a contradiction because $B \subseteq \mathrm{End}_A M$.

Let $M = M_0 \supset M_1 \supset \cdots \supset M_t = 0$ be a composition series for M as an $A \otimes_C B^{\mathrm{op}}$-module. Then $\mathrm{Ann}(M_i/M_{i+1}) = P_i$ is a primitive ideal of $A \otimes_C B^{\mathrm{op}}$ and $P_1 \cdots P_{i-1} = 0$. However, $A \otimes_C B^{\mathrm{op}}$ is prime so that one of the P must be (0) and the Proposition is established.

Using the Proposition and Theorem 1 we can now state a criterion for the primitivity of $D[X_1, \cdots, X_n]$.

THEOREM 2. *$D[X_1, \cdots, X_t]$ is primitive if and only if $M_n(D)$, some n, contains a subfield of transcendence t over C, the center of D.*

PROOF. If $M_n(D)$ contains the function field $C(X_1, \cdots, X_t)$, where (X_i) are algebraically independent, then, in the Proposition, take $A = D$, and $B = C[X_1, \cdots, X_t] \subseteq \mathrm{End}_D(D^{(n)}) \cong M_n(D)$ where $D^{(n)}$ is an n-dimensional vector space over D, and the primitivity of $D[X_1, \cdots, X_t]$ follows immediately.

For the converse, suppose $R = D[X_1, \cdots, X_t]$ is primitive and R/L is faithful and simple, then $L \cap C[X_1, \cdots, X_t] = 0$ because L cannot contain central elements, and so $C[X_1, \cdots, X_t]$ embeds in $\mathrm{End}_R(R/L)$, a division ring. Hence the rational field $C(X_1, \cdots, X_t)$ is contained in $\mathrm{End}_R(R/L)$ which is in $\mathrm{End}_D(R/L) = M_n(D)$ for some n, by Theorem 1.

4. The Example

R. Resco [3] has shown that if A is a central simple C-algebra containing the rational function field $C(y_1, \cdots, y_t)$, then the global dimension (right or left) of the polynomials in $x_1, \cdots, x_t$, t commutative indeterminates localized at the central polynomials, is at least t. Denote this ring by $A(X_1, \cdots, X_t)_C$; then $\mathrm{gl.\,dim}\, A(X_1, \cdots, X_t)_C \geqq t$.

Let $D^{(n)}$ denote the division ring of fractions of A_n, the n-th Weyl algebra over a field C of characteristic zero. It is trivial that $M_m(D^{(n)})$, for all m, contains subfields of transcendence degree at least n over C. On the other hand, if $M_m(D^{(n)})$ contains a subfield of transcendence degree ν, we get by Resco's result that $\mathrm{gl.\,dim}\, M_m(D^{(n)})(X_1, \cdots, X_\nu)_C \geqq \nu$. However,

$$\text{gl. dim}\, M_m\,(D^{(n)})(X_1,\cdots,X_\nu)_C = \text{gl. dim}\, M_m\,(D^{(n)}(X_1,\cdots,X_\nu)_C)$$
$$= \text{gl. dim}\, D^{(n)}(X_1,\cdots,X_\nu)_C.$$

But $D^{(n)}(X_1,\cdots,X_\nu)_C$ is a ring of fractions of $A_n(X_1,\cdots,X_\nu)_C$ which is isomorphic with the n-th Weyl algebra A_n over the rational field $C(X_1,\cdots,X_\nu)$. The latter has gl. dim $= n$ ([4]), and thus we have proved that

$$\nu \leqq \text{gl. dim}\, M_m\,(D^{(n)})(X_1,\cdots,X_\nu)_C \leqq \text{gl.}\, A_n\,(C(X_1,\cdots,X_\nu)) = n.$$

Hence the maximal $\nu = n$, i.e. the maximum transcendence degree of a subfield of $M_m(D^{(n)})$ for arbitrary m is n, and we have by Theorem 2

THEOREM 3. *The ring $D^{(n)}[X_1,\cdots,X_t]$, $1 \leqq t \leqq n$ is primitive, but for $t > n$ it is not primitive.*

Resco's result answers also positively, for certain division rings, the following interesting question, in the way we have done for $D = D^{(n)}$:

Let D be a division ring with the center C. If t is the maximum transcendence degree over C of the commutative subfields of D, is t also the maximum transcendence degree of the subfields of $M_n(D)$, for all n?

The case $t = 0$ means that if D is algebraic over C, is also $M_n(D)$ algebraic over C, which is a famous problem for which we have a positive answer only for uncountable C ([1]). The question we proposed before is a natural extension of this problem, and it remains open even for uncountable fields C.

REFERENCES

1. S. A. Amitsur, *Algebras over infinite fields*, Proc. Amer. Soc. 7 (1956), 35–48.
2. J. Diximier, *Algebras Enveloppantes*, Paris, 1974.
3. R. Resco, Thesis, University of California, San Diego, 1978, to be published.
4. J. E. Roos, *Determination de la dimension homologique globale des algèbres de Weyl*, C. R. Acad. Sci., Ser. A, **274** (1972), 23–26.

THE HEBREW UNIVERSITY OF JERUSALEM
JERUSALEM, ISRAEL

AND

UNIVERSITY OF CALIFORNIA
SAN DIEGO
LA JOLLA, CALIF. 92093 USA