Canad. Math. Bull. Vol. 14 (3), 1971

SETS OF GENERATORS OF A COMMUTATIVE AND ASSOCIATIVE ALGEBRA(1)

BY
D. Ž. DJOKOVIĆ

ABSTRACT. Let A be a finite dimensional commutative and associative algebra with identity, over a field K. We assume also that A is generated by one element and consequently, isomorphic to a quotient algebra of the polynomial algebra $K[X]$. If $A=K[a]$ and $b_i=f_i(A)$, $f_i(X) \in K[X]$, $1 \le i \le r$ we find necessary and sufficient conditions which should be satisfied by $f_i(X)$ in order that $A=K[b_1, \ldots, b_r]$.
The result can be stated as a theorem about matrices. As a special case we obtain a recent result of Thompson [4].
In fact this last result was established earlier by Mirsky and Rado [3]. I am grateful to the referee for supplying this reference.

1. In this note K will denote a field and X an indeterminate over K. Let A be an associative algebra over K. If $S \subset A$ then S^* will denote the subalgebra of A generated by S. If A has identity element 1_A we define

$$K[S] = (S \cup \{1_A\})^* = S^* + K1_A.$$

LEMMA 1. *Let A be a finite dimensional associative K-algebra with identity. Assume that there exists $a \in A$ such that $A=K[a]$ and, consequently, A is commutative. Let*

$$m(X) = (X-\lambda)^m, \lambda \in K, m > 1$$

be the minimal polynomial of a.

If $b=f(a), f(X) \in K[X]$ then $\{b\}^* = \operatorname{rad} A$ if and only if $f(\lambda)=0$ and $f'(\lambda) \neq 0$.

Proof. We can assume that $\lambda=0$. Necessity. If $f(0)\neq 0$ then $b=f(a) \notin \operatorname{rad} A$. Hence, we must have $f(0)=0$. Since $a \in \operatorname{rad} A$ we have $a=g(b)=g(f(a))$ for some $g(X) \in K[X]$. If follows that

$$X = g(f(X)) + X^m h(X)$$

for some $h(X) \in K[X]$. Differentiating and evaluating at $X=0$ we get $1=g'(f(0))f'(0)$ and so $f'(0) \neq 0$.

Sufficiency. We have an isomorphism

$$\theta : A \to K[X]/(X^m)$$

Received by the editors February 3, 1970 and, in revised form, December 16, 1970.
(1) The preparation of this paper was supported in part by National Research Council Grant A-5285.

such that

$$\theta(a) = \bar{X} = X+(X^m).$$

We find

$$\begin{aligned}\theta(b) &= \theta(f(a)) = f(\theta(a)) = f(\bar{X}) = \overline{f(X)} \\ &= f'(0)\bar{X}+\overline{g(X)}\end{aligned}$$

where $g(x) \in K[X]$ is divisible by X^2.

It follows that $\theta(b), \theta(b)^2, \ldots, \theta(b)^{m-1}$ are linearly independent. This implies that also $b, b^2, \ldots, b^{m-1}$ are linearly independent. Since $b \in \operatorname{rad} A$ and $\dim \operatorname{rad} A = m-1$ we must have $\{b\}^* = \operatorname{rad} A$.

THEOREM 1. *Let A be a finite dimensional associative K-algebra with identity. Let $A = K[a]$ for some $a \in A$ which implies that A is commutative. Let*

$$m(X) = \prod_{i=1}^{k} m_i(X)$$

be the minimal polynomial of a where

$$m_i(X) = (X-\lambda_i)^{m_i}, \quad m_i \geq 1$$

and $\lambda_i \in K$ are distinct.

Let $b_i = f_i(a), f_i(X) \in K[X], 1 \leq i \leq r$. Then $A = K[b_1, \ldots, b_r]$ if and only if the following two conditions are satisfied:

(i) *If $i \neq j$ there exists s such that $f_s(\lambda_i) \neq f_s(\lambda_j)$,*

(ii) *If $m_i > 1$ there exists t such that the derivative $f_t'(\lambda_i) \neq 0$.*

Proof. Necessity. If $A = K[b_1, \ldots, b_r]$ there exists a polynomial F over K such that

$$a = F(b_1, \ldots, b_r) = F(f_1(a), \ldots, f_r(a)).$$

Hence,

$$X = F(f_1(X), \ldots, f_r(X)) + m(X)f(X)$$

for some $f(X) \in K[X]$. This identity implies both conditions (i) and (ii).

Sufficiency. The algebra A has decomposition into direct sum of ideals (see [2, p. 64])

$$A = \bigoplus_{i=1}^{k} A_i$$

such that

$$A_i \cong K[X]/(m_i(X)).$$

An element $x \in A$ is in the ideal A_j if and only if $x = f(a), f(X) \in K[X]$ implies that

$$f(X) \equiv 0 (\bmod m_i(X)), \quad i \neq j.$$

For fixed $i \geq 2$ let $g_i(X) = f_s(X)$ where s is such that $f_s(\lambda_i) \neq f_s(\lambda_1)$. Such s exists by (i). Let

$$\psi_i(X) = \frac{g_i(X) - g_i(\lambda_i)}{g_i(\lambda_1) - g_i(\lambda_i)},$$

$$\psi(X) = \prod_{i=2}^{k} \psi_i(X)^{m_i}.$$

If $m_1 > 1$ let

$$\phi(X) = [f_t(X) - f_t(\lambda_1)]\psi(X)$$

where t is such that $f_t'(\lambda_1) \neq 0$.

Such t exists by (ii).

We have $\psi(a), \phi(a) \in K[b_1, \ldots, b_r]$ and

$$\psi(X) \equiv 0 (\bmod m_i(X)), \quad i \geq 2$$
$$\phi(X) \equiv 0 (\bmod m_i(X)), \quad i \geq 2$$
$$\psi(\lambda_1) = 1, \phi(\lambda_1) = 0, \phi'(\lambda_1) \neq 0.$$

These conditions imply that $\psi(a), \phi(a) \in A_1$. If $m_1 = 1$ then $A_1 \subset K[b_1, \ldots, b_r]$ because $\psi(a) \neq 0$ and $\dim A_1 = 1$. If $m_1 > 1$ then by Lemma 1

$$K[\phi(a)] = \operatorname{rad} A_1.$$

Since $\psi(\lambda_1) \neq 0$ we have $\psi(a) \notin \operatorname{rad} A_1$ and consequently

$$K[\phi(a), \psi(a)] = A_1.$$

In both cases $A_1 \subset K[b_1, \ldots, b_r]$. Similarly we can prove that $A_i \subset K[b_1, \ldots, b_r]$ for $i \geq 2$.

Theorem 1 is proved.

Now we extend Theorem 1 to the case when the roots of $m(X)$ are not necessarily in K.

THEOREM 2. *Let A be a finite dimensional associative K-algebra with identity. Let $A = K[a]$ for some $a \in A$ which implies that A is commutative. Let*

$$m(X) = \prod_{i=1}^{k} (X - \lambda_i)^{m_i}, \quad m_i \geq 1$$

be the minimal polynomial of a, where $\lambda_i \in L$, L an extension field of K, and λ_i, $1 \leq i \leq k$ are distinct.

Let $b_i = f_i(a)$, $f_i(X) \in K[X]$, $1 \leq i \leq r$. Then $A = K[b_1, \ldots, b_r]$ if and only if the conditions (i) *and* (ii) *of Theorem* 1 *are satisfied.*

https://doi.org/10.4153/CMB-1971-058-7 Published online by Cambridge University Press

Proof. Tensor product $L \otimes_K A$ is an associative L-algebra with identity. The equality

$$A = K[b_1, \ldots, b_r]$$

is obviously equivalent to

$$L \otimes A = L[1 \otimes b_1, \ldots, 1 \otimes b_r].$$

We still have

$$1 \otimes b_i = f_i(1 \otimes a), \quad 1 \leq i \leq r.$$

Hence, we can apply Theorem 1.

2. In this section we apply Theorem 2 to the algebra $M_n(K)$ of $n \times n$ matrices over K.

THEOREM 3. *Let $A \in M_n(K)$ and $B_i = f_i(A)$, $f_i(X) \in K[X]$, $1 \leq i \leq r$. Let $m(X)$ be the minimal polynomial of A and*

$$m(X) = \prod_{i=1}^{k} (X - \lambda_i)^{m_i}, \quad m_i \geq 1$$

where $\lambda_i \in L$, L an extension field of K, and λ_i are distinct. Then

$$K[A] = K[B_1, \ldots, B_r]$$

if and only if the conditions (i) *and* (ii) *of Theorem* 1 *are satisfied.*

Proof. The algebra $K[A]$ is of the type considered in Theorem 2. The case $r = 1$ of Theorem 3 was proved recently by Thompson [4].

REMARK 1. If $A, B \in M_n(K)$, $f(X) \in K[X]$ and $B = f(A)$ then Theorem 1 of [3] (i.e. case $r = 1$ of our Theorem 3) gives necessary and sufficient conditions for the existence of $g(X) \in K[X]$ such that $A = g(B)$. These conditions are expressed in terms of $f(X)$ and the minimal polynomial $m(X)$ of A.

More generally, if $A, B \in M_n(K)$ one can give necessary and sufficient conditions for existence of $f(X) \in K[X]$ such that $B = f(A)$. These conditions can be easily obtained from [1, p. 158, Theorem 9]. They will be expressed in terms of elementary divisors of A and B.

REMARK 2. One can generalize the problem, for instance, as follows. Let I be an ideal of the polynomial algebra $K[X_1, \ldots, X_n]$ in n indeterminates X_i, $1 \leq i \leq n$, over a field K. Let A be the factor algebra $K[X_1, \ldots, X_n]/I$. The problem is to characterize the family of finite sets of generators of A. We have solved this problem for $n = 1$. The case $n > 1$ seems to be much more difficult to answer.

References

1. F. R. Gantmacher, *The theory of matrices*, Vol. 1, Chelsea, New York, 1960.

2. S. Lang, *Algebra*, Addison Wesley, New York, 1965.

3. L. Mirsky and R. Rado, *A note on matrix polynomials*, Quart. J. Math. Oxford Ser. (2) **8** (1957), 128–132.

4. R. C. Thompson, *On the matrices A and $f(A)$*, Canad. Math. Bull. **12** (1969), 581–587.

University of Waterloo,
Waterloo, Ontario