DIVISORS OF ZERO IN MATRIC RINGS

NEAL H. MCCOY

1. **Introduction.** An element a of a ring S is a *divisor of zero* in S if there exists a nonzero element x of S such that $ax=0$, or a nonzero element y of S such that $ya=0$. The purpose of the present note is to obtain several theorems about divisors of zero in matric rings which, although quite elementary in character, have apparently not been previously noted. Throughout, unless otherwise stated, R will be used to denote an arbitrary commutative ring with unit element. Let R_n denote the ring of all matrices of order n with elements in R, and $R[\lambda]$ the ring of polynomials in the indeterminate λ with coefficients in R. If A is an element of R_n, we shall denote by $f(\lambda)=|\lambda-A|$ the *characteristic polynomial* of A, and thus $f(\lambda)$ is an element of $R[\lambda]$, with leading coefficient 1. The ideal $\mathfrak{m}$ of all elements $g(\lambda)$ such that $g(A)=0$ is the *minimum ideal* of A. If the minors of $\lambda-A$ of order $n-1$ are denoted by $h_{ij}(\lambda)$ $(i, j=1, 2, \cdots, n)$, it has been shown in a previous paper[1] that $g(\lambda)\equiv 0$ $(\mathfrak{m})$, if and only if

$$g(\lambda)h_{ij}(\lambda) \equiv 0 \quad (f(\lambda)), \qquad i, j = 1, 2, \cdots, n.$$

If $R[A]$ denotes the subring of R_n generated by A together with the unit element of R_n, which we identify with the unit element of R, then the elements of $R[A]$ are the polynomials in A with coefficients in R. It is quite easy to show that A is a divisor of zero in R_n if and only if $|A|$ is a divisor of zero in R. But we shall show, in §2, that A is actually a divisor of zero in $R[A]$ if it is a divisor of zero in R_n—a fact which is almost trivial if R is a field. This theorem is used in the following section in which we define, by means of the Sylvester determinant, the *resultant* $\mathfrak{R}(f, g)$ of two elements $f(\lambda)$ and $g(\lambda)$ of $R[\lambda]$ and show, following Frobenius, that if $f(\lambda)$ has leading coefficient unity,

$$\mathfrak{R}(f, g) = |g(A)|,$$

where A is *any* matrix having $f(\lambda)$ as characteristic polynomial. It then follows readily that an element $g(\lambda)$ of $R[\lambda]$ is *prime to*[2] $\mathfrak{m}$ if and

[1] Neal H. McCoy, *Concerning matrices with elements in a commutative ring*, this Bulletin, vol. 45 (1939), pp. 280–284. Hereafter, this paper will be referred to as M.

[2] For definitions of this term, see W. Krull, *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, Mathematische Annalen, vol. 101 (1929), pp. 729–744. This will be referred to later as K. A definition will also be found in §3 of the present paper.

only if it is prime to $f(\lambda)$, which in turn is true if and only if $\mathfrak{R}(f,g)$ is not a divisor of zero in R.

If A is such that $\mathfrak{m}=(f(\lambda))$, we may say, following Sylvester, that A is *not derogatory*. Let us, as above, denote the minors of $\lambda-A$ of order $n-1$ by $h_{ij}(\lambda)$, and set

$$\mathfrak{a} = (h_{11}(\lambda), h_{12}(\lambda), \cdots, h_{nn}(\lambda)).$$

We conclude our remarks by showing that, if each ideal in R has a finite basis, A is not derogatory if and only if $\mathfrak{a}$ contains an element of R which is not a divisor of zero in R.

2. **Divisors of zero in $R[A]$.** We shall now prove

THEOREM 1. *An element A of R_n is a divisor of zero in $R[A]$ if and only if $|A|$ is a divisor of zero in R.*

The necessity follows easily by a familiar argument. Suppose that A is a divisor of zero in $R[A]$ and hence that there exists a nonzero element X of $R[A]$ such that $AX=0$. In other words, if $A=(a_{ij})$, the following system of equations,

$$\sum_{j=1}^{n} a_{ij}x_j = 0, \qquad i = 1, 2, \cdots, n,$$

has a solution $(\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n)$ in R with some $\bar{x}_\alpha \neq 0$. Multiply these equations in order by the respective cofactors of $a_{1\alpha}, a_{2\alpha}, \cdots, a_{n\alpha}$ in $|A|$, and add. There results $\bar{x}_\alpha |A| = 0$, and hence $|A|$ is a divisor of zero in R.

We now pass to the second part of the proof. Accordingly, we assume that there is an element $k \neq 0$ of R such that $k|A| = 0$, and shall show that A is a divisor of zero in $R[A]$. Our method is to assume that A is not a divisor of zero in $R[A]$ and obtain a contradiction.

First, we prove the following

LEMMA. *If B and C are elements of R_n and k is an element of R such that $kB=kC$, then $k|B| = k|C|$.*

This follows from the fact that $kb_{ij}=kc_{ij}$, where $B=(b_{ij})$ and $C=(c_{ij})$, together with the following calculation. If $b=b_{i_11}b_{i_22}\cdots b_{i_nn}$ is any term, except possibly for sign, in the expansion of $|B|$, and $c=c_{i_11}c_{i_22}\cdots c_{i_nn}$ the corresponding term in the expansion of $|C|$, then

$$\begin{aligned} kb &= (kb_{i_11})b_{i_22}\cdots b_{i_nn} = (kc_{i_11})b_{i_22}\cdots b_{i_nn} \\ &= c_{i_11}(kb_{i_22})b_{i_33}\cdots b_{i_nn} = c_{i_11}c_{i_22}(kb_{i_33})\cdots b_{i_nn}, \end{aligned}$$

and a continuation of this process shows finally that this is equal to kc.

We now turn to the proof of Theorem 1. The matrix A satisfies its characteristic equation,[3] and hence there is a relation of the form

$$A^n + a_1A^{n-1} + \cdots + a_n = 0, \tag{1}$$

where $a_n = \pm |A|$, and thus $ka_n = 0$. Hence, from (1), we get an equation of the form

$$kA(A^{n-1} + a_1A^{n-2} + \cdots + a_{n-1}) = 0.$$

But, by our assumption that A is not a divisor of zero in $R[A]$, it follows that

$$k(A^{n-1} + a_1A^{n-2} + \cdots + a_{n-1}) = 0, \tag{2}$$

or, as we may write it,

$$kA(A^{n-2} + a_1A^{n-3} + \cdots + a_{n-2}) = -ka_{n-1}.$$

Now, applying the lemma, we see that

$$k|A| \cdot |A^{n-2} + a_1A^{n-3} + \cdots + a_{n-2})| = k(-1)^n a_{n-1}^n.$$

But $k|A| = 0$, and therefore $ka_{n-1}^n = 0$. Suppose $ka_{n-1}^j \neq 0$, but $ka_{n-1}^{j+1} = 0$ $(j \geqq 0)$. Then $k' = ka_{n-1}^j \neq 0$ has the property that $k'a_n = k'a_{n-1} = 0$, and hence from (2),

$$k'A(A^{n-2} + \cdots + a_{n-2}) = 0.$$

A repetition of this argument shows that there is an element $k'' \neq 0$ of R, which is a multiple of k', such that $k''a_n = k''a_{n-1} = k''a_{n-2} = 0$. Continuing this process we finally get an element $l \neq 0$ of R such that $lA = 0$, which violates our assumption that A is not a divisor of zero in $R[A]$. The theorem is therefore established.

Our method of proof also establishes the following

COROLLARY. *If A is a divisor of zero in R_n, there exists an element $g(A)$ of $R[A]$ such that*

$$Ag(A) = 0, \qquad g(A) \neq 0,$$

where $g(\lambda)$ is an element of $R[\lambda]$ with the property that, for some positive integer i,

$$\lambda^i g(\lambda) = kf(\lambda),$$

$f(\lambda)$ being the characteristic polynomial of A and k an element of R.

[3] See M, p. 282.

3. **Resultants and their properties.** We first make some preliminary remarks.[4] Let $\mathfrak{a}$ be an ideal in the commutative ring R, with unit element. An element b of R is said to be *prime to* $\mathfrak{a}$ if $bx \equiv 0$ $(\mathfrak{a})$ implies that $x \equiv 0$ $(\mathfrak{a})$, otherwise b is *not prime to* $\mathfrak{a}$. An element b is prime to the element a if b is prime to the principal ideal (a). If every element of an ideal $\mathfrak{b}$ is not prime to $\mathfrak{a}$, but every proper divisor of $\mathfrak{b}$ contains an element prime to $\mathfrak{a}$, then $\mathfrak{b}$ is necessarily a prime ideal which we shall call a *maximal prime ideal belonging to* $\mathfrak{a}$. Krull has shown, by methods which are necessarily transfinite if R is unrestricted, that every ideal has maximal prime ideal divisors and that *the elements of R which are not prime to* $\mathfrak{a}$ *are precisely the elements which are contained in some maximal prime ideal belonging to*[5] $\mathfrak{a}$.

We now consider the ring $R[\lambda]$, where λ is an indeterminate, and let

$$f(\lambda) = \lambda^n + a_1\lambda^{n-1} + \cdots + a_n, \qquad g(\lambda) = b_0\lambda^m + b_1\lambda^{m-1} + \cdots + b_m$$

be two elements of $R[\lambda]$, the leading coefficient of $f(\lambda)$ being 1. In case R is a field, the vanishing of the resultant of $f(\lambda)$ and $g(\lambda)$ furnishes a necessary and sufficient condition that $f(\lambda)$ and $g(\lambda)$ be not prime to each other.[6] We shall now obtain an analogous result in case R is unrestricted.

Let us denote the resultant of $f(\lambda)$ and $g(\lambda)$ by $\mathfrak{R}(f, g)$ and define it in a purely formal way by the Sylvester determinant

$$\mathfrak{R}(f, g) = \begin{vmatrix} 1 & a_1 & \cdot & \cdot & \cdot & a_n & & \\ & 1 & a_1 & \cdot & \cdot & \cdot & a_n & \\ & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & 1 & a_1 & \cdot & \cdot & \cdot & a_n \\ b_0 & b_1 & \cdot & \cdot & \cdot & b_m & & \\ & b_0 & b_1 & \cdot & \cdot & \cdot & b_m & \\ & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & b_0 & b_1 & \cdot & \cdot & \cdot & b_m \end{vmatrix},$$

the blank spaces consisting of zeros.

The connection with the preceding part of the paper is indicated by

[4] Cf. K, p. 732.

[5] In fact, it can be shown that if in R every ideal has a finite basis, the maximal prime ideals belonging to a are precisely the maximal among the prime ideals associated with the primary ideals in a normalized decomposition of $\mathfrak{a}$ into the intersection of primary ideals. All of these prime ideals are the *prime ideals belonging to* $\mathfrak{a}$.

[6] In case R is a field, this implies that $f(\lambda)$ and $g(\lambda)$ have a common factor of degree at least one.

THEOREM 2. *If A is any element of R_n which has characteristic polynomial $f(\lambda)$, then*

$$\mathfrak{R}(f, g) = |g(A)|. \tag{3}$$

This is an almost immediate consequence of Frobenius' theorem for the case in which R is the field of complex numbers.[7] For if we consider the elements of a matrix A, as well as the coefficients of $g(\lambda)$ to be independent complex variables, relation (3) is seen to be an identity in these variables and thus remains true if these variables are replaced by elements of[8] R.

Now let A be any fixed element of R_n with characteristic polynomial $f(\lambda)$. The ideal $\mathfrak{m}$ of all elements $h(\lambda)$ of $R[\lambda]$ such that $h(A)=0$ is the minimum ideal of A. It is now clear that an element $g(\lambda)$ of $R[\lambda]$ is prime to $\mathfrak{m}$ if and only if $g(A)$ is not a divisor of zero in $R[A]$, and Theorem 1 states that this is the case if and only if $|g(A)|$ is not a divisor of zero in R. We shall now prove

THEOREM 3. *An element $g(\lambda)$ of $R[\lambda]$ is prime to $\mathfrak{m}$ if and only if it is prime to $f(\lambda)$.*

By the preceding remarks, and Theorem 2, we see that $g(\lambda)$ is prime to $\mathfrak{m}$ if and only if $\mathfrak{R}(f, g)$ is not a divisor of zero in R. But clearly $\mathfrak{R}(f, g)$ depends only on $f(\lambda)$ and $g(\lambda)$ and not on the particular choice of matrix A with characteristic polynomial $f(\lambda)$. Let A' be a matrix with characteristic polynomial $f(\lambda)$, and such that its minimum ideal is[9] $\mathfrak{m}'=(f(\lambda))$. Then $g(\lambda)$ is prime to $\mathfrak{m}'$ if and only if $\mathfrak{R}(f, g)$ is not a divisor of zero in R. But it was found above that this is precisely the condition that $g(\lambda)$ be prime to $\mathfrak{m}$, and the theorem is established.

Since $g(\lambda)$ is prime to $\mathfrak{m}$ if and only if $\mathfrak{R}(f, g)$ is not a divisor of zero in R, we have incidentally proved the following result which is independent of the theory of matrices:

THEOREM 4. *If R is a commutative ring with unit element and λ is an indeterminate, an element $g(\lambda)$ of $R[\lambda]$ is prime to the element $f(\lambda)$, with leading coefficient unity, if and only if $\mathfrak{R}(f, g)$ is not a divisor of zero in R.*

4. **A characterization of matrices which are not derogatory.** Let

[7] G. Frobenius, *Ueber lineare Substitutionen und bilineare Formen*, Journal für die reine und angewandte Mathematik, vol. 84 (1878), p. 11.

[8] Cf. M, p. 281.

[9] This will certainly be the case if A' is the companion matrix of $f(\lambda)$. See relation (4) of §4.

A be an element of R_n, with characteristic polynomial $f(\lambda)$ and minimum ideal $\mathfrak{m}$. Following Sylvester, we may say that A is *not derogatory* if $\mathfrak{m}=(f(\lambda))$. Let $h_{ij}(\lambda)$ denote the minors of $\lambda-A$ of order $n-1$. It was remarked above that an element $g(\lambda)$ of $R[\lambda]$ is an element of $\mathfrak{m}$ if and only if

$$g(\lambda)h_{ij}(\lambda) \equiv 0 \quad (f(\lambda)), \qquad i, j = 1, 2, \cdots, n. \tag{4}$$

We shall now make use of this fact in a proof of the following theorem:

THEOREM 5. *If in R each ideal has a finite basis, the matrix A is not derogatory if and only if the ideal*

$$\mathfrak{a} = (h_{11}(\lambda), h_{12}(\lambda), \cdots, h_{nn}(\lambda))$$

contains an element of R which is not a divisor of zero.

Suppose b is an element of R which is not a divisor of zero and that $b\equiv 0$ $(\mathfrak{a})$. Then, from (4), it follows that if $g(\lambda)\equiv 0$ $(\mathfrak{m})$, then $bg(\lambda)\equiv 0$ $(f(\lambda))$. But $f(\lambda)$ has leading coefficient 1, and from this fact, and the fact that b is not a divisor of zero, an easy calculation shows that $g(\lambda)\equiv 0$ $(f(\lambda))$. Since always $f(\lambda)\equiv 0$ $(\mathfrak{m})$, this shows that A is non-derogatory.

Now let us assume that A is not derogatory which means that $g(\lambda)\mathfrak{a}\equiv 0$ $(f(\lambda))$ implies that $g(\lambda)\equiv 0$ $(f(\lambda))$. Under hypothesis of a finite basis for each ideal in R, this means that $\mathfrak{a}$ is not divisible by any prime ideal belonging to[10] $(f(\lambda))$. This implies, in turn, that there is an element $q(\lambda)$ of $\mathfrak{a}$ which is not in any prime ideal belonging to $(f(\lambda))$ and is thus prime to[11] $f(\lambda)$. But since $q(\lambda)$ is prime to $f(\lambda)$, it follows by Theorem 4 that $\mathfrak{R}(f, q)=|q(A)|$ is not a divisor of zero in R. Let $|q(A)|=a$. Extend R to a ring R' consisting of elements of the form r/a^i $(i=0, 1, \cdots; r \text{ in } R)$.[12] In R', a has an inverse and therefore $q(A)$ has an inverse[13] which is a polynomial in A with coefficients in R', say

$$p(A) = (b_0/a^{i_0})A^k + (b_1/a^{i_1})A^{k-1} + \cdots + (b_k/a^{i_k}).$$

Since $q(A)p(A)=1$, in R we have a relation of the form

$$q(A)(c_0A^k + c_1A^{k-1} + \cdots + c_k) = a^l = b,$$

[10] Cf. van der Waerden, *Moderne Algebra*, vol. 2, p. 41.

[11] In fact, it may be shown by induction on k that if every element of an ideal $\mathfrak{a}$ is contained in some one of the prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_k$, then $\mathfrak{a}$ is divisible by some one of the $\mathfrak{p}_i$.

[12] See R. Holzer, *Zur Theorie der primären Ringe*, Mathematische Annalen, vol. 96 (1927), p. 722.

[13] Cf. M, p. 282.

where b is not a divisor of zero. If we set

$$t(\lambda) = c_0\lambda^k + c_1\lambda^{k-1} + \cdots + c_k,$$

we have in $R[\lambda]$

$$q(\lambda)t(\lambda) \equiv b \quad (\mathfrak{m}),$$

which, by hypothesis, implies that

$$q(\lambda)t(\lambda) \equiv b \quad (f(\lambda)).$$

Now $q(\lambda) \equiv 0$ $(\mathfrak{a})$ and clearly also $f(\lambda) \equiv 0$ $(\mathfrak{a})$, from which it follows that $b \equiv 0$ $(\mathfrak{a})$. The theorem is therefore established.

SMITH COLLEGE