JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematical Sciences
Vol. 75B, Nos. 1 and 2, January–June 1971

On the Smith Normal Form

Morris Newman

Institute for Basic Standards, National Bureau of Standards, Washington, D.C. 20234

(October 21, 1970)

An elementary proof is given of the fact that if A, B are nonsingular $n \times n$ matrices over a principal ideal ring R, then the kth invariant factor of AB is divisible by the kth invariant factor of A and by the kth invariant factor of B, $1 \leq k \leq n$. Some consequences are drawn.

Key words: Invariant factors; principal ideal rings, Smith normal form.

1. Introduction

Let R be a principal ideal ring (a commutative ring with identity 1 in which every ideal is principal). If $A \epsilon R_n$ (the ring of $n \times n$ matrices over R) A^T will denote its transpose. If in addition A is nonsingular then

$$S(A) = \operatorname{diag}(s_1(A), s_2(A), \ldots, s_n(A))$$

will denote the Smith normal form of A (see [2] for an excellent reference on this topic). It is well-known that if A, B are nonsingular elements of R_n then the determinantal divisors of AB are divisible by the corresponding determinantal divisors of A and of B. It is not so well-known that the same result is true for the invariant factors: i.e., $s_k(AB)$ is divisible by $s_k(A)$ and by $s_k(B)$, $1 \leq k \leq n$. An interesting consequence is that $S(AB) = S(A)S(B)$, provided that A, B have relatively prime determinants. This result is a consequence of a rather general theorem about rings which is given by Kaplansky in his paper [1].[1] Since Kaplansky did not include a proof of his theorem in his paper, and since the proof at any rate would be ring-theoretic, it is desirable to have a purely elementary matrix-theoretic proof, and this is what is given here.

We also note that the result concerning the determinantal divisors follows as a corollary, since if A is nonsingular then its kth determinantal divisor $d_k(A)$ is just $s_1(A)s_2(A) \ldots s_k(A)$, $1 \leq k \leq n$.

2. A Lemma

We first prove the following lemma:

LEMMA 1: *Suppose that* $\begin{pmatrix} \mathrm{H} & 0 \\ 0 & \mathrm{K} \end{pmatrix}$ *is a nonsingular element of* R_n *which is in Smith normal form. Let* m *be any non-zero element of* R *and suppose that there is a matrix* U *of* R_n *such that* (det U, m) = 1, *and*

$$\mathrm{U}\begin{pmatrix} \mathrm{H} & 0 \\ 0 & \mathrm{K} \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix} \bmod \mathrm{m}. \tag{1}$$

AMS Subject Classification: Primary 15A33, Secondary 15A21.

[1] Figures in brackets indicate the literature references at the end of this paper.

422-795 O - 71 - 6

Then K $\equiv 0$ mod m.

PROOF: Put

$$H = \text{diag }(h_1, h_2, \ldots, h_r), K = \text{diag }(k_1, k_2, \ldots, k_s),$$

where $r+s=n$ and $h_i | h_{i+1} (1 \leq i \leq r-1)$, $k_j | k_{j+1} (1 \leq j \leq s-1)$, $h_r | k_1$. Partition U so that

$$U = \begin{pmatrix} U_1 & U_2 \\ U_3 & U_4 \end{pmatrix},$$

where U_1 is $r \times r$, U_4 $s \times s$. Then (1) implies that

(2) $$U_3 H \equiv 0 \qquad \text{mod } m,$$

(3) $$U_4 K \equiv 0 \qquad \text{mod } m.$$

We can multiply (2) on the right by diag $(h_r/h_1, h_r/h_2, \ldots, 1)$ to obtain

$$h_r U_3 \equiv 0 \qquad \text{mod } m.$$

Put

(4) $$(h_r, m) = \delta.$$

Then

$$\frac{h_r}{\delta} U_3 \equiv 0 \qquad \text{mod } \frac{m}{\delta},$$

and since $(h_r/\delta, m/\delta) = 1$,

(5) $$U_3 \equiv 0 \qquad \text{mod } \frac{m}{\delta}.$$

Now set $K = k_1 K'$, where $K' = \text{diag }(1, k_2/k_1, \ldots, k_s/k_1)$. Then from (3),

$$k_1 U_4 K' \equiv 0 \qquad \text{mod } m.$$

Put

(6) $$(k_1, m) = \Delta.$$

Then as before we deduce that

(7) $$U_4 K' \equiv 0 \qquad \text{mod } \frac{m}{\Delta}.$$

Now $\delta | \Delta$, in virtue of (4), (6), and the fact that $h_r | k_1$. It follows that $m/\Delta | m/\delta$, and so (5) holds modulo m/Δ as well. Thus

$$U = \begin{pmatrix} U_1 & U_2 \\ U_3 & U_4 \end{pmatrix} \equiv \begin{pmatrix} U_1 & U_2 \\ 0 & U_4 \end{pmatrix} \qquad \text{mod } \frac{m}{\Delta},$$

$$\det U \equiv \det U_1 \det U_4 \text{ mod } \frac{m}{\Delta}.$$

Since $(\det U, m)=1$, it follows that $(\det U_4, m/\Delta)=1$. Hence (7) implies that $K' \equiv 0 \bmod m/\Delta$, and so $\Delta \equiv 0 \bmod m$, since the 1,1 element of K' is 1. Thus (6) implies that $m|k_1$, and the conclusion follows.

3. The Theorems

We are now prepared to use Lemma 1. Let A, B be nonsingular elements of R_n. Then matrices U, C of R_n exist such that U is a unit matrix and

$$US(AB)=S(A)C. \tag{8}$$

Certainly $s_1(A)$ divides $s_1(AB)$, since $s_1(A)$ is the greatest common divisor of the elements of A and $s_1(AB)$ the greatest common divisor of the elements of AB. For $2 \leq k \leq n-1$, choose $m=s_k(A)$ and apply Lemma 1. We are left with $k=n$. Write $U=(u_{ij}), C=(c_{ij})$. Then (8) implies that

$$u_{ij}s_j(AB)=c_{ij}s_i(A),$$

so that for $i=n$,

$$u_{nj}s_j(AB) \equiv 0 \bmod s_n(A).$$

Since $s_j(AB)\,|\,s_n(AB), 1 \leq j \leq n$, this implies that

$$u_{nj}s_n(AB) \equiv 0 \bmod s_n(A).$$

The fact that $s_n(A)\,|\,s_n(AB)$ now follows, since $(u_{n1}, u_{n2}, \ldots, u_{nn})=1$.

If we note that in addition $S(A^T)=S(A)$, the entire argument may also be applied to the pair B^T, A^T, and we finally obtain

THEOREM 1: *Let* A, B *be nonsingular elements of* R_n. *Then* $s_k(AB)$ *is divisible by* $s_k(A)$ *and by* $s_k(B)$ *for* $1 \leq k \leq n$.

From this theorem we easily deduce

THEOREM 2: *Suppose that* A, B *are elements of* R_n *with relatively prime determinants. Then*

$$S(AB)=S(A)S(B).$$

PROOF: Since $(\det A, \det B)=1$ and $s_k(A)\,|\det A$, $s_k(B)\,|\det B$, it follows that $(s_k(A), s_k(B))=1$ for $1 \leq k \leq n$. Then Theorem 1 implies that

$$s_k(AB) \equiv 0 \bmod s_k(A)s_k(B), 1 \leq k \leq n.$$

But $\prod_{k=1}^{n} s_k(AB)$ is a unit multiple of $\det(AB)$, and $\prod_{k=1}^{n} s_k(A)s_k(B)$ is a unit multiple of $\det A \det B$. It follows that $s_k(AB)|s_k(A)s_k(B)$ is a unit for $1 \leq k \leq n$. But this implies that in fact $s_k(AB)= s_k(A)s_k(B)$ for $1 \leq k \leq n$, since associated elements in corresponding diagonal positions of matrices in Smith normal form must be equal. This completes the proof.

4. Concluding Remarks

Theorem 2 is definitely false if $(\det A, \det B) > 1$. Thus if m is any element of R, and

$$A=\begin{pmatrix}1 & 1\\ 0 & m\end{pmatrix}, \quad B=\begin{pmatrix}1 & 0\\ -1 & m\end{pmatrix},$$

then

$$S(A) = S(B) = \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix},$$

but

$$S(AB) = \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}.$$

This example also shows that $S(AB)$ need not equal $S(BA)$, since here

$$S(BA) = \begin{pmatrix} 1 & 0 \\ 0 & m^2 \end{pmatrix}.$$

However, $S(AB)$ and $S(BA)$ are equal if A and B have relatively prime determinants as is readily seen from Theorem 2.

A simple example illustrating the use to which Theorem 1 may be put is furnished by choosing A as the incidence matrix of a finite projective plane of order n, so that A is a $v \times v$ rational integral matrix satisfying

$$AA^T = A^TA = nI + J,$$

where $v = n^2 + n + 1$ and J is the matrix all of whose entries are 1. It is easy to show that the invariant factors of $nI + J$ are

$$1(\text{once}),\ n(v-2 \text{ times}),\ n(n+1)^2(\text{once}).$$

Thus if the Smith normal form of A is

$$S(A) = \operatorname{diag}(\alpha_1, \alpha_2, \ldots, \alpha_v),$$

then

$$\alpha_1 = 1,\ \alpha_i | n(2 \leqslant i \leqslant v-1),\ \alpha_v | n(n+1)^2.$$

Now the facts that

$$\alpha_1\alpha_2 \ldots \alpha_v = n^{\frac{v-1}{2}}(n+1),$$

and $(\alpha_i, n+1) = 1$ for $1 \leqslant i \leqslant v-1$, imply that $\alpha_v = (n+1)\alpha_v'$, where now

$$\alpha_1\alpha_2 \ldots \alpha_{v-1}\alpha_v' = n^{\frac{v-1}{2}},$$

$$\alpha_i | \alpha_{i+1} (1 \leqslant i \leqslant v-2),\ \alpha_{v-1} | \alpha_v',\ \alpha_v' | n.$$

Choosing n square-free, we easily obtain

COROLLARY 1: *Let* A *be the incidence matrix of a finite projective plane of order* n, *where* n *is square-free. Then the invariant factors of* A *are*

$$1\left(\frac{n^2+n}{2} + 1 \textit{ times}\right),\ n\left(\frac{n^2+n}{2} - 1 \textit{ times}\right),\ n(n+1)\,(\textit{once}).$$

Of course such a matrix is known to exist only if n is a prime, and this result might possibly be of some use in settling the question of existence for other square-free values of n.

5. References

[1] Kaplansky, I., Elementary divisors and modules, Trans. Amer. Math. Soc. **66,** 464–491 (1949).

[2] MacDuffee, C. C., The theory of matrices, Reprint of first edition, (Chelsea, New York, 1964).

(Paper 75B1&2–347)