JOURNAL OF RESEARCH of the National Bureau of Standards — B. Mathematical Sciences
Vol. 76B, Nos. 3 and 4, July–December 1972

A Note on the Multiplicative Property of the Smith Normal Form*

Marvin Marcus and Ernest E. Underwood*****

(September 21, 1972)

This paper contains an elementary proof of the fact that if A and B are n-square matrices over a principal ideal domain R with relatively prime determinants, then $S(AB)=S(A)S(B)$ where $S(A)$ is the Smith normal form of A.

Key words: Compound; divisors; matrix.

In [2; p. 33][1] the following interesting result appears: *If* A *and* B *are* n*-square matrices over a principal ideal domain* R *and* g.c.d. (det (A), det (B))=1 *then* S(AB)=S(A)S(B) *where* S(A) *is the Smith normal form of* A.

The purpose of this note is to present a simple proof of the result that uses elementary properties of compound matrices.

LEMMA. *Let* $Q=\text{diag}\,(q_1, \ldots, q_n)$, $P=\text{diag}\,(p_1, \ldots, p_n)$, $q_1 \mid q_j$, $p_1 \mid p_j$, $j=1, \ldots, n$ *and* g.c.d. $(p_i, q_j)=1$, $i, j=1, \ldots, n$. *Let* U *be an* n*-square matrix with the property that* g.c.d. $(u_{11}, u_{21}, \ldots, u_{n1})=$ g.c.d. $(u_{11}, u_{12}, \ldots, u_{1n})=1$. *Then the* g.c.d. *of all the entries in* QUP *is* p_1q_1.

PROOF. Obviously $p_1q_1|QUP$, i.e., p_1q_1 divides every entry of QUP. Write $QUP=p_1q_1D$. Suppose that $p|D$ where p is a prime. It is simple to see that the first row and column of D are respectively

$$D_{(1)}=[u_{11}, u_{12}p_2', \ldots, u_{1n}p_n'], \qquad p_i'=p_ip_1^{-1},$$

and

$$D^{(1)}=[u_{11}, q_2'u_{21}, \ldots, q_n'u_{n1}], \qquad q_i'=q_iq_1^{-1}.$$

Now $p|D_{(1)}$ and since g.c.d.$(u_{11}, \ldots, u_{1n})=1$ we conclude that $p|p_k'$, for some $k=2, \ldots, n$. Similarly $p|D^{(1)}$ so $p|q_l'$ for some $l=2, \ldots, n$. But then $p|p_k'|p_k$, $p|q_l'|q_l$ and this contradicts g.c.d.$(p_k, q_l)=1$.

Since A and $S(A)$ are equivalent it follows immediately that AB and $S(A)US(B)$ are equivalent where U is unimodular. Thus

$$S(AB)=S(S(A)US(B)). \tag{1}$$

Since it is obvious that $d_k(S(A)S(B))=d_k(A)d_k(B)$, $k=1, \ldots, n$, we need only show that

$$d_k(A)d_k(B)=d_k(S(A)US(B)), k=1, \ldots, n,$$

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

*An invited paper. The research of the first author was supported by U.S. Air Force Office of Scientific Research Grant AFOSR 72-2164, and the research of both authors was supported under the auspices of An Intermediate Short Course in Linear Algebra for College Teachers of Mathematics, N.S.F. Grant GY9414.

**Present address: Department of Mathematics, University of California, Santa Barbara, California 93106.
***Present address: Department of Mathematics, Utah State University, Logan, Utah 84321.

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

to complete the proof.

If $C_k(X)$ denotes the kth compound of the matrix X [1; p. 16] then we immediately have

$$C_k(S(A)US(B))=C_k(S(A))C_k(U)C_k(S(B)) \tag{2}$$

and the matrix $C_k(U)$ is unimodular. For, $C_k(UV)=C_k(I_n)$ implies $C_k(U)C_k(V)=C_k(I_n)$ and thus $C_k(U)$ has an inverse over R if U does. (Or more simply, apply the Sylvester-Franke theorem to see that $C_k(U)$ has a unit determinant.) Hence the entries in the first row (column) of $C_k(U)$ are relatively prime. The divisibility properties of the determinantal divisors together with the hypothesis that g.c.d. $(d_n(A), d_n(B))=1$ imply that any two main diagonal elements of the diagonal matrices $C_k(S(A))$ and $C_k(S(B))$ are relatively prime. Moreover the 1,1 entry of $C_k(S(A))$ is $d_k(A)$ and similarly for $C_k(S(B))$. We can now apply the lemma to the matrix on the right in (2) to conclude that $d_k(A)d_k(B)$ is the g.c.d. of the entries in $C_k(S(A))C_k(U)C_k(S(B))$; i.e., $d_k(A)d_k(B)$ is the g.c.d. of the entries in $C_k(S(A)US(B))$. But in view of (1),

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

and the proof is complete.

References

[1] Marcus, Marvin, and Minc, Henryk, A Survey of Matrix Theory and Matrix Inequalities, (Allyn and Bacon, Boston, Mass., 1964).

[2] Newman, Morris, Integral Matrices, (Academic Press, New York, 1972).

(Paper 76B3&4–373)