PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 86, Number 1, September 1982

AN INEQUALITY FOR INVARIANT FACTORS

ROBERT C. THOMPSON

ABSTRACT. A divisibility relation is proved connecting the invariant factors of integral matrices A, B, C when $C = AB$.

Let A, B, and C be $n \times n$ matrices with entries in a principal ideal domain $\mathfrak{R}$, and with $C = AB$. In a recent note [3] on the multiplicative property of the Smith normal form, Morris Newman observed the fact: if $d_i(A)$ denotes the ith determinantal divisor of A, then $d_i(A)d_i(B) \mid d_i(C)$, where $\mid$ denotes divisibility. The objective of this paper is to prove the following divisibility property of invariant factors, a property containing Newman's observation as a special case.

Notation. $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_n$, $\beta_1 \mid \beta_2 \mid \cdots \mid \beta_n$, $\gamma_1 \mid \gamma_2 \mid \cdots \mid \gamma_n$ are the invariant factors of A, B, and C, respectively. See [4] for all properties of invariant factors used here.

THEOREM. *We have*

$$(1) \qquad \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_m}\beta_{j_1}\beta_{j_2}\cdots\beta_{j_m} \mid \gamma_{i_1+j_1-1}\gamma_{i_2+j_2-2}\cdots\gamma_{i_m+j_m-m}$$

whenever the integer subscripts satisfy

$$1 \leqslant i_1 < i_2 < \cdots < i_m, \quad 1 \leqslant j_1 < j_2 < \cdots < j_m, \quad i_m + j_m \leqslant m + n.$$

PROOF. Let p be a fixed prime in $\mathfrak{R}$, and let $\mathfrak{R}_p$ be the ring of all fractions a/b, where a, b lie in $\mathfrak{R}$ and p does not divide b. Ring $\mathfrak{R}_p$ is a principal ideal ring, with every nontrivial ideal a power of the principal ideal generated by p. Observe that (1) holds when the α's, β's, and γ's are invariant factors if and only if it holds when the α's, β's, and γ's are the elementary divisors belonging to the prime p, for each choice of p dividing $\det C$. And these elementary divisors are the invariant factors of A, B, C when the matrices are regarded as having elements in the local ring $\mathfrak{R}_p$, an observation due some years ago to L. Gerstein [1]. So (1) will be proved if it can be proved when A, B, and C are matrices over $\mathfrak{R}_p$.

The proof will easily be completed once the following lemma is established.

LEMMA. *Over $\mathfrak{R}_p$, we may assume that*:

(i) *B is diagonal*, $B = \operatorname{diag}(\beta_1, \beta_2, \ldots, \beta_n)$,

(ii) *A is triangular*, $A = [a_{ij}]$ *with* $a_{ij} = 0$ *for* $i > j$,

(iii) *C is triangular*, $C = [c_{ij}]$ *with* $c_{ij} = 0$ *for* $i > j$, *and* $c_{ii} = \gamma_i$, $c_{ii} \mid c_{ij}$ *for* $j > i$, $1 \leqslant i \leqslant n$.

Received by the editors September 15, 1981.
1980 *Mathematics Subject Classification.* Primary 15A36; Secondary 15A39.

0002-9939/82/0000-0194/$02.00

PROOF OF LEMMA. From $C = AB$ we get $UCV = (UAW^{-1})(WBV)$, where U, V, W are unimodular. First, choose W and V to put B into its Smith form: $WBV = \operatorname{diag}(\beta_1, \beta_2, \ldots, \beta_n)$. Then choose U to put AW^{-1} into Hermite (triangular) form. Since we are only interested in invariant factors, which these transformations preserve, we may henceforth assume that B is diagonal, A and C are triangular. All of this holds over $\mathfrak{R}$ as well as over $\mathfrak{R}_p$.

If $C = 0$, the claims are trivially correct, so suppose that $C \neq 0$.

Always γ_1 is the greatest common divisor of the c_{ij}, but over $\mathfrak{R}_p$ γ_1 is the power of p exactly present in those c_{ij} exhibiting the lowest exponent on p. Among these minimal c_{ij}, select one with i least. If $i > 1$ we may left multiply C and A by a unimodular U that adds row i to row 1. For the $C = AB$ now at hand, the minimal p power exactly dividing an element of C appears in a first row element. So we may suppose that $i = 1$. If the minimal c_{1j} for which j is least has $j > 1$, proceed as follows: Choose unimodular V such that in CV column j of C is added to column 1, and let W be unimodular so that in WB the β_j/β_1 multiple of row 1 is subtracted from row j. Then in $CV = (AW^{-1})(WBV)$, we have $WVB = \operatorname{diag}(\beta_1, \ldots, \beta_n)$ and γ_1 (to within a unit) is the (1, 1) element of CV. But CV and AW^{-1} are no longer triangular.

Rename the matrices at hand as $C = AB$, with $c_{11} = \gamma_1$ and $B = \operatorname{diag}(\beta_1, \ldots, \beta_n)$. Since $c_{i1} = a_{i1}\beta_1$ and $c_{11} \mid c_{i1}$, evidently $a_{11} \mid a_{i1}$. Elementary row operations on A (therefore on C also) now make $a_{21} = \cdots = a_{n1} = 0$, whence $c_{21} = \cdots = c_{n1} = 0$. Thus A and C are block triangular, and $c_{11} = \gamma_1$ divides each c_{ij}. Since C is unimodularly equivalent to the direct sum of c_{11} and $[c_{ij}]_{2 \leq i,j \leq n}$, evidently the trailing $(n-1)$-square block in C has invariant factors $\gamma_2, \ldots, \gamma_n$. And by an obvious left multiplication by a unimodular U, the trailing blocks in A and C may be assumed triangular.

We now repeat this procedure on the last $n - 1$ rows and columns if the trailing block in C is nonzero, there being nothing further to prove if it is zero. Continuing in this manner, the lemma is established.

PROOF OF THEOREM CONCLUDED. We proceed by induction on n. The initial value is $n = m$, in which case (1) merely asserts that $\det A \det B \mid \det C$, trivially true. So suppose $n > m$.

We adapt a trick used by M. F. Smiley [5] in quite another context. Define integers u and v by

$$i_1 = 1, \ldots, i_u = u, \qquad u = m \quad \text{or} \quad i_{u+1} > u + 1,$$
$$j_1 = 1, \ldots, j_v = v, \qquad v = m \quad \text{or} \quad j_{v+1} > v + 1.$$

One of u, v is the smaller, and by transposing C if necessary we may assume that $v \leq u$. Now apply the lemma and so have $B = \operatorname{diag}(\beta_1, \ldots, \beta_n)$, A and C triangular, $c_{ii} = \gamma_i$ and $c_{ii} \mid c_{ij}$ for all $i \leq j$.

Let C' be the matrix gotten from C by deleting row $v + 1$ and column $v + 1$; similarly for A', B' from A and B, respectively. The diagonal form of B then implies that $C' = A'B'$, and that the invariant factors of B' are

$$\beta'_1 = \beta_1, \ldots, \beta'_v = \beta_v, \qquad \beta'_{v+1} = \beta_{v+2}, \ldots, \beta'_{n-1} = \beta_n.$$

The invariant factors $\alpha'_1 \mid \cdots \mid \alpha'_{n-1}$ of A' are known [6] to satisfy

$$\alpha_1 \mid \alpha'_1, \ldots, \alpha_{n-1} \mid \alpha'_{n-1}.$$

And the special structure of C shows that the invariant factors of C' are

$$\gamma'_1 = \gamma_1, \ldots, \gamma'_v = \gamma_v, \qquad \gamma'_{v+1} = \gamma_{v+2}, \ldots, \gamma'_{n-1} = \gamma_n.$$

Let

$$I_1 = i_1, \ldots, I_m = i_m,$$
$$J_1 = j_1, \ldots, J_v = j_v, \quad J_{v+1} = j_{v+1} - 1, \ldots, J_m = j_m - 1.$$

By induction on n, the inequality

$$\alpha'_{I_1} \cdots \alpha'_{I_m} \beta'_{J_1} \cdots \beta'_{J_m} \mid \gamma'_{I_1+J_1-1} \cdots \gamma'_{I_m+J_m-m} \tag{2}$$

holds. However, the relations written down in the last several lines show that (2) implies (1).

COMMENTS. The inequality just proved is one of a large family in which the indices are Littlewood-Richardson sequences. The entire family was established some years ago by the present author, but never published, using a method based on results of Klein [2]. Since the inequality (1) is so clean, and its proof so elementary, it seems worthwhile to publish it separately.

The special case $\alpha_i \beta_j \mid \gamma_{i+j-1}$ was used in [7] and proved there by a method somewhat similar to the one used above. This special case can be shown to imply the multiplicative property of the Smith form, that is, $S(AB) = S(A)S(B)$ when A and B have relatively prime determinants; $S(A)$ is the Smith form of A. See [7] for details.

The role of Littlewood-Richardson sequences in some of the classical eigenvalue problems of linear algebra was described in [8].

ACKNOWLEDGEMENT. The preparation of this paper was partly supported by AFOSR Grant 79-0127.

REFERENCES

1. L. Gerstein, *A multiplicative property of invariant factors*, Linear and Multilinear Algebra **2** (1974), 141–142.

2. T. Klein, *The multiplication of Schur functions and extensions of p-modules*, J. London Math. Soc. **43** (1968), 280–284.

3. M. Newman, *A result about determinantal divisors*, Linear and Multilinear Algebra (to appear).

4. ______, *Integral matrices*, Academic Press, New York, 1972.

5. M. F. Smiley, *Inequalities related to Lidskii's*, Proc. Amer. Math. Soc. **19** (1968), 1029–1034.

6. R. C. Thompson, *Interlacing inequalities for invariant factors*, Linear Algebra Appl. **24** (1979), 1–31.

7. ______, *Left multiples and right divisors of integral matrices* (submitted).

8. ______, *Eigenvalues, singular values, and number theory*, Santa Barbara Conference on Matrix Theory, 1977.

ALGEBRA INSTITUTE AND DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT SANTA BARBARA, SANTA BARBARA, CALIFORNIA 93106