The Smith Form, the Inversion Rule for 2×2 Matrices, and the Uniqueness of the Invariant Factors for Finitely Generated Modules

Robert C. Thompson
Algebra Institute and
Mathematics Department
University of California at Santa Barbara
Santa Barbara, California, 93106

Submitted by G. P. Barker

Lat $\mathfrak{R}$ be a commutative integral domain. Suppose that

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

is a partitioned $2n \times 2n$ matrix over $\mathfrak{R}$ with $n \times n$ blocks. Further, assume that M is unimodular, so that it has an inverse

$$N = M^{-1} = \begin{bmatrix} P & Q \\ R & S \end{bmatrix}$$

with entries from $\mathfrak{R}$ (and $n \times n$ blocks). When the blocks are scalars, i.e., when $n = 1$, the inversion rule for 2×2 matrices shows that

A and S are associates, B and Q are associates,
C and R are associates, D and P are associates.

In this paper we first generalize this 2×2 inversion rule to larger blocks, $n \times n$ blocks with arbitrary n. Next, we indicate an application of the resulting theorem to the least-common-left-multiple–greatest-common-right-divisor theory of integral matrices. Then we consider the connection between our theorem and the invariant factor theory for finitely generated $\mathfrak{R}$-modules, and we shall establish this surprising fact: Our block 2×2 inversion theorem is logically equivalent to the uniqueness part of the invariant factor theorem for $\mathfrak{R}$-modules.

NOTATION. The Smith form of an $\mathfrak{R}$ matrix K will be denoted by $\mathfrak{S}(K)$. See [1], [2], [3], or [4] for a discussion of the Smith form.

52 Vanderbilt Ave., New York, NY 10017 0024-3795/82/030197+5$02.75

THEOREM 1. *When matrix M is unimodular, with square blocks as above, the Smith forms of the blocks in M and in $N = M^{-1}$ are related by the rule for inverting 2×2 matrices:*

$$\mathbb{S}(A)=\mathbb{S}(S), \qquad \mathbb{S}(B)=\mathbb{S}(Q),$$

$$\mathbb{S}(C)=\mathbb{S}(R), \qquad \mathbb{S}(D)=\mathbb{S}(P).$$

Proof. Various proofs can be given; the following is as simple as any. We shall show that A and S have the same determinantal divisors by proving that each $r\times r$ minor in A is a linear combination of $r\times r$ minors from S, then reversing the roles of A and S; $1\leqslant r\leqslant n$. Passing to P_1MP_2, where P_1 and P_2 are block diagonal permutation matrices, we may suppose that the $r\times r$ minor in question from A sits in leading position. By the well-known identity linking minors of M and M^{-1}, this leading $r\times r$ minor of A equals a unit multiple of the trailing $(2n-r)$-square minor in N. Expand this latter minor of N by Laplace across its last n rows. Each $n\times n$ determinant Δ in this expansion formed from the last n rows of N also uses some set of columns, of which at most $n-r$ lie outside S. Therefore, at least r lie inside S. Expand Δ along any set of r columns lying inside S. Doing this for each Δ, we find that the original $r\times r$ minor from A equals a linear combination of $r\times r$ minors from S. This proves that $\mathbb{S}(A)=\mathbb{S}(S)$, and the other parts of the theorem are proved similarly. ■

REMARK. The theorem is false if M is not assumed to be unimodular.

APPLICATION. If a and b are nonzero scalars (elements of $\mathfrak{R}$), their greatest common divisor (a,b) and their least common multiple $\langle a,b\rangle$ may always be chosen so that

$$\langle a,b\rangle=\frac{ab}{(a,b)}.$$

When A and B are invertible matrices over $\mathfrak{R}$, they possess a greatest common right divisor (A,B) and a least common left multiple $\langle A,B\rangle$. A natural question to ask is whether the above scalar formula extends to full size matrices. It does, it being always possible to choose (A,B) and $\langle A,B\rangle$ so that

$$\langle A,B\rangle=A(A,B)^{-1}B.$$

The proof of this interesting fact is in [5], its key step being an application of Theorem 1. The reader may consult [5] for details.

We now turn to the connection with module theory, and we must first review some facts about finitely generated $\mathfrak{R}$-modules [1]. Let $\mathfrak{M}$ be a finitely generated $\mathfrak{R}$-module, and $m_1,\ldots,m_n$ a set of generators. For notational convenience, we form $m_1,\ldots,m_n$ into a column n-tuple $m=[m_1,\ldots,m_n]^{\mathsf{T}}$. The symbols x, y, z, t will denote row tuples with elements from $\mathfrak{R}$.

A (possibly rectangular) matrix M over $\mathfrak{R}$ is a complete relations matrix for the generators m_i if (i) $Mm=0$, (ii) $xm=0$ implies $x=yM$ for an appropriate y. A standard fact is that a complete relations matrix always exists. It is not unique; if U is unimodular, then UM is another. Choosing U to put M into triangular (Hermite) form, we find a complete relations matrix with at most n nonzero rows. Adding or deleting zero rows, we are entitled to assume that the complete relations matrix is square, and we henceforth make this restriction. If U and V are unimodular, UMV is a complete relations matrix for the generators in $V^{-1}m$. Choosing U,V to put M into Smith form, we deduce that $\mathfrak{M}$ is a direct sum of cyclic modules, with the order ideals of the cyclic generators forming a divisibility chain. These are called the invariant factors for $\mathfrak{M}$, and a basic question is: are they unique? Conceivably, uniqueness could fail in either of two ways: (i) a different complete relations matrix for m could yield a different set of invariant factors; (ii) a different set of generators could lead to a different set of invariant factors. However, (i) cannot lead to nonuniqueness, since if M and M_1 are complete relations matrices for m, then $M=XM_1$ and $M_1=YM$ for matrices X,Y over $\mathfrak{R}$. Thus M and M_1 have the same determinantal divisors and therefore the same invariant factors. The rest of this paper explores point (ii).

It will be convenient below to (possibly) adjoin additional zero generators to the m_i. Then the new complete relations matrix is a direct sum of M and an identity matrix, the invariant factors undergo adjunction by (1)'s and the cyclic decomposition of $\mathfrak{M}$ is unaffected, only zero direct summands being added.

Let finitely many elements b_i of $\mathfrak{M}$ be given. We adjoin zero elements to the b_i or to the m_i, as necessary, to ensure that there are the same number of b_i as m_i. Let $b=[b_1,\ldots,b_n]^{\mathsf{T}}$. Since the m_i generate, $b=Xm$ for some $n\times n$ matrix X over $\mathfrak{R}$.

LEMMA. *The elements of b generate $\mathfrak{M}$ if and only if the left ideal (X, M) in matrix $n\times n$ space equals the unit ideal (I_n).*

Proof. Suppose the elements of b generate $\mathfrak{M}$. Then $m=Yb$ for some matrix Y, hence $(I-YX)m=0$, and therefore $I-YX=ZM$ for some matrix Z over $\mathfrak{R}$. Thus $(X, M)=(I)$. The converse reverses these steps, using also $Mm=0$. ∎

THEOREM 2. *Let the elements of* $b = Xm$ *generate* $\mathfrak{M}$, *and let* P *be a unimodular* $2n \times 2n$ *matrix bringing* $\begin{bmatrix} M \\ X \end{bmatrix}$ *to a left Hermite form* $\begin{bmatrix} H \\ 0 \end{bmatrix}$, *i.e.*,

$$P\begin{bmatrix} M \\ X \end{bmatrix} = \begin{bmatrix} H \\ 0 \end{bmatrix} \qquad \text{with} \quad P = \begin{bmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{bmatrix}, \tag{1}$$

and $n \times n$ *blocks. Set*

$$Q = P^{-1} = \begin{bmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{bmatrix}.$$

Then: Q_{11} *is a complete relations matrix for the elements of* m, *and* P_{22} *is a complete relations matrix for the elements of* b.

Proof. From (1) we get $H = P_{11}M + P_{12}X$ and $M = Q_{11}H$, $X = Q_{21}H$. (Also, $P_{21}M + P_{22}X = 0$.) Thus the left ideal $(X, M) = (H)$. Since this ideal is the unit ideal, H must be unimodular, and therefore is the identity matrix, since it is in Hermite form. We show that P_{22} is a complete relations matrix for b. First: $P_{22}b = P_{22}Xm = -P_{21}Mm = 0$. Hence P_{22} is a relations matrix. Suppose that $tb = 0$. Thus $tXm = 0$, hence $tX = zM$ for some z, and thus (using $H = I$)

$$0 = [z, -t]\begin{bmatrix} M \\ X \end{bmatrix} = [z, -t]\begin{bmatrix} Q_{11} \\ Q_{21} \end{bmatrix}.$$

Hence $[z, -t]Q = [0, w]$ for some w. But then $[z, -t] = [0, w]P$, so that $-t = wP_{22}$. Therefore P_{22} is complete. The fact that Q_{11} is a complete relations matrix for b follows from the formula $M = Q_{11}$ established earlier in the proof. ■

We now establish the link between Theorem 1 and module theory.

THEOREM 3. *The truth of Theorem* 1 *is logically equivalent to the uniqueness part of the invariant factor theorem for finitely generated* $\mathfrak{R}$*-modules.*

Proof. Assume the truth of Theorem 1. Then P_{22} and Q_{11} have the same invariant factors; hence the invariant factors do not depend on the choice of generators m, b of the $\mathfrak{R}$-module.

Suppose now that Theorem 1 is false. Then a unimodular matrix P would exist such that the blocks P_{22} in P and Q_{11} in $Q = P^{-1}$ have different invariant factors. Form an R-module $\mathfrak{M}$ with n generators m_i and Q_{11} as a complete relations matrix. (This always exists: Take the $\mathfrak{R}$-module $\mathfrak{F}$ on free generators m_i', form the submodule $\mathfrak{S}$ generated by the elements of $Q_{11}m'$, let $\mathfrak{M} = \mathfrak{F}/\mathfrak{S}$, and take m_i to be the homomorphic image of m_i'.) Set $X = Q_{21}$, and put $b = Xm$. Thus, with $M = Q_{11}$, (1) holds with $H = I$. Then (X, M) is the unit ideal, so that the elements of b generate. By the proof of Theorem 2, P_{22} is a complete relations matrix for these generators, and thus the nonuniqueness of the module invariant factors is evident. ■

The preparation of this note was partially supported by U.S. Air Force Grant No. 79-0127.

REFERENCES

1 N. Jacobson, *Basic Algebra I*, Freeman, San Francisco, 1974.
2 C. C. MacDuffee, *The Theory of Matrices*, Chelsea, New York, 1956.
3 M. Newman, *Integral Matrices*, Academic, New York, 1972.
4 M. Marcus, *Introduction to Modern Algebra*, Dekker, New York, 1978.
5 R. C. Thompson, Left multiples and right divisors of integral matrices, submitted for publication.

Received 10 August 1981