

MATRIX COMPLETION THEOREMS¹

MORRIS NEWMAN

ABSTRACT. Let R be a principal ideal ring, $M_{t,n}$ the set of $t \times n$ matrices over R . The following results are proved:

(a) Let $D \in M_{n,n}$. Then the least nonnegative integer t such that a matrix $\begin{bmatrix} * & * \\ * & D \end{bmatrix}$ exists which belongs to $\text{GL}(n+t, R)$ is $t = n - p$, where p is the number of invariant factors of D equal to 1.

(b) Any primitive element of $M_{1,2n}$ may be completed to a $2n \times 2n$ symplectic matrix.

(c) If $A, B \in M_{n,n}$ are such that $[A, B]$ is primitive and AB^T is symmetric, then $[A, B]$ may be completed to a $2n \times 2n$ symplectic matrix.

(d) If $A \in M_{t,t}$, $B \in M_{t,n-t}$ are such that $[A, B]$ is primitive and A is symmetric, then $[A, B]$ may be completed to a symmetric element of $\text{SL}(n, R)$, provided that $1 \leq t \leq n/3$.

(e) If $n \geq 3$, then any primitive element of $M_{1,n}$ occurs as the first row of the commutator of two elements of $\text{SL}(n, R)$.

1. Introduction. In this paper we consider matrices over a principal ideal ring and the problem of completing, or embedding, such matrices so that the resulting matrices satisfy certain given criteria. We let R denote an arbitrary principal ideal ring and define $M_{t,n} = M_{t,n}(R)$, the set of $t \times n$ matrices over R , $M_n = M_n(R)$, the set of $n \times n$ matrices over R . As usual, $\text{GL}(n, R)$ will denote the group of unit (or unimodular) matrices of M_n , and $\text{SL}(n, R)$ the subgroup of $\text{GL}(n, R)$ consisting of the matrices of determinant 1. We also let $\text{Sp}(2n, R)$ denote the subgroup of symplectic matrices of $\text{SL}(2n, R)$, defined as the automorphs of the matrix $K = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$, where $I = I_n$ is the $n \times n$ identity matrix. Equivalently, if $S = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, where $A, B, C, D \in M_n$, then S is symplectic if and only if $AD^T - BC^T = I$, and AB^T, CD^T are symmetric. $\text{Sp}(2n, R)$ is, in general, a subgroup of infinite index of $\text{SL}(2n, R)$, although $\text{Sp}(2, R) = \text{SL}(2, R)$.

Suppose $1 \leq t \leq n$. The element α of $M_{t,n}$ is said to be *primitive* if $d_t(\alpha) = 1$, where $d_t(\alpha)$ is the t th determinantal divisor of α . The following result and its generalization are the basis of the entire theory of matrix equivalence.

BASIC RESULT. *Let α be a primitive element of $M_{1,n}$. Then an element of $\text{GL}(n, R)$ exists whose first row is α . If $n \geq 2$, an element of $\text{SL}(n, R)$ exists whose first row is α .*

Received by the editors May 10, 1984.

1980 *Mathematics Subject Classification.* Primary 15A36, 15A33, 15A21.

¹ The preparation of this paper was supported by a grant from the National Science Foundation.

©1985 American Mathematical Society
0002-9939/85 \$1.00 + \$.25 per page

GENERALIZATION. Suppose $1 \leq t \leq n$. Let α be a primitive element of $M_{t,n}$. Then an element of $GL(n, R)$ exists whose first t rows coincide with α . If $t < n$, an element of $SL(n, R)$ exists whose first t rows coincide with α .

Thus, such an α may always be completed to a unimodular matrix. For a convenient reference on matrix equivalence, see [1 or 2].

2. Statement of results. We prove a number of completion theorems concerned with block matrices, symplectic matrices, symmetric matrices, matrix commutators, and, of course, unimodular matrices. The theorems to be proved fall in the following categories.

Block completions.

THEOREM 1. Let $D \in M_n$. Let t be the least nonnegative integer such that matrices A, B, C exist with $A \in M_t$, $B \in M_{t,n-t}$, $C \in M_{n-t,t}$, and $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \in GL(n+t, R)$. Then $t = n - p$, where p is just the number of ones in the Smith normal form of D .

Symplectic completions.

THEOREM 2. Let $\tau \in M_{1,2n}$ be primitive. Then τ may be completed to an element of $Sp(2n, R)$.

THEOREM 3. Let $A, B \in M_n$, and suppose $[A, B]$ is primitive and AB^T is symmetric. Then $[A, B]$ may be completed to an element of $Sp(2n, R)$.

This theorem is not new. It was first proved by C. L. Siegel [5, p. 592] in connection with his work on the applications of the symplectic group to number theory; a generalization (with a different proof) was given by I. Reiner in [4]. The proof given here is totally different from either of these proofs and very simple, so we include it.

Symmetric completions. It was shown in [3] that if $n \geq 3$ and α is any primitive element of $M_{1,n}$, then α may be completed to a symmetric element of $SL(n, R)$. This result was used to prove certain factorization theorems for the elements of $SL(n, R)$ in terms of symmetric matrices. Theorem 5 below generalizes this result and is based on the following

THEOREM 4. Let $A \in M_p$, $B \in M_{p,q}$, $A = A^T$. Assume that $[A, B]$ is primitive. Then matrices Y, Z exist such that $Y \in M_{q,p}$, $Z \in M_p$, $Z = Z^T$, and

$$M = \begin{bmatrix} A & -BY \\ -Y^T B^T & Z \end{bmatrix} \in GL(2p, R).$$

THEOREM 5. Suppose $1 \leq t \leq n/3$. Let $A \in M_t$, $B \in M_{t,n-t}$, $A = A^T$. Assume that $[A, B]$ is primitive. Then $[A, B]$ may be completed to a symmetric element of $SL(n, R)$.

The result is false, in general, if it is only assumed that $1 \leq t \leq n/2$. This leaves the question of determining those t for which the result is true.

Matrix commutators.

THEOREM 6. Suppose $n \geq 3$. Let α be a primitive element of $M_{1,n}$. Then matrices A, B of $SL(n, R)$ exist such that the first row of $ABA^{-1}B^{-1}$ is α .

3. Proofs.

PROOF OF THEOREM 1. First note that $\begin{bmatrix} 0 & I \\ I & D \end{bmatrix}$ is a $2n \times 2n$ completion, so that $t \leq n$. Furthermore, if $p = n$, then D is already unimodular and $t = 0$ in this case. Thus, we may assume $p < n$. We may also assume that D is in Smith normal form; for if $U, V \in \text{GL}(n, R)$, then

$$\begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix} \begin{bmatrix} * & * \\ * & D \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & V \end{bmatrix} = \begin{bmatrix} * & * \\ * & UDV \end{bmatrix},$$

and the matrices

$$\begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}, \quad \begin{bmatrix} I & 0 \\ 0 & V \end{bmatrix}$$

are unimodular.

Let s_1, s_2, \dots, s_n denote the invariant factors of D . Then

$$D = \begin{bmatrix} I_p & 0 \\ 0 & E \end{bmatrix},$$

where E is in Smith normal form and satisfies $E \equiv 0 \pmod{s_{p+1}}$.

Suppose now that

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

is unimodular. Partition M in accordance with the partition imposed by D , so that

$$M = \begin{bmatrix} A & B_1 & B_2 \\ C_1 & I_p & 0 \\ C_2 & 0 & E \end{bmatrix} \equiv \begin{bmatrix} A & B_1 & B_2 \\ C_1 & I_p & 0 \\ C_2 & 0 & 0 \end{bmatrix} \pmod{s_{p+1}}.$$

The matrix B_2 is a $t \times (n - p)$ matrix, and if $t < n - p$, then $\det(M) \equiv 0 \pmod{s_{p+1}}$. Hence, a necessary condition for M to be unimodular is that $t \geq n - p$. We need only show, therefore, that $t = n - p$ will suffice. This is clear, however, since we may choose $A = 0$, $B_1 = 0$, $B_2 = I_{n-p}$, $C_1 = 0$, $C_2 = I_{n-p}$; whence

$$M = \begin{bmatrix} 0 & 0 & I_{n-p} \\ 0 & I_p & 0 \\ I_{n-p} & 0 & E \end{bmatrix}$$

is clearly unimodular. This completes the proof.

PROOF OF THEOREM 2. We may assume that $n > 1$, since the theorem is known and trivial for $n = 1$. We use the fact that if S is any element of $\text{Sp}(2n, R)$, then τ has a symplectic completion if and only if τS has a symplectic completion. Write $\tau = [\alpha; \beta]$, where $\alpha, \beta \in M_{1,n}$. Choose $U \in \text{GL}(n, R)$ so that βU is in Hermite normal form. Then

$$M = \begin{bmatrix} (U^T)^{-1} & 0 \\ 0 & U \end{bmatrix}$$

is symplectic, and $\tau M = [*; \beta U]$. Hence, we may assume

$$(1) \quad \beta = [\beta_1, 0, \dots, 0].$$

Now suppose that $\alpha = [\alpha_1, \alpha_2, \dots, \alpha_n]$. Choose $V \in GL(n-1, R)$ so that $[\alpha_2, \dots, \alpha_n]V$ is in Hermite normal form, and put

$$W = [1] + V, \quad N = \begin{bmatrix} W & 0 \\ 0 & (W^T)^{-1} \end{bmatrix}.$$

Then N is symplectic, and $[\alpha; \beta]N = [\alpha W; \beta(W^T)^{-1}] = [\alpha W; \beta]$ because of (1). This allows us to assume that

$$(2) \quad \alpha = [\alpha_1, \alpha_2, 0, \dots, 0].$$

Let E_{ij} denote (as usual) the matrix which has a 1 in the (i, j) position and 0 elsewhere. Then if x, y are arbitrary elements of R , the matrices

$$S(x) = \begin{bmatrix} I & 0 \\ xE_{11} & I \end{bmatrix}, \quad W(y) = \begin{bmatrix} I & yE_{11} \\ 0 & I \end{bmatrix}$$

are symplectic; and

$$\begin{aligned} [\alpha; \beta]S(x) &= [\alpha_1 + x\beta_1, \alpha_2, 0, \dots, 0; \beta_1, 0, \dots, 0], \\ [\alpha; \beta]W(y) &= [\alpha_1, \alpha_2, 0, \dots, 0; \beta_1 + y\alpha_1, 0, \dots, 0]. \end{aligned}$$

This sets up a euclidean algorithm, and after finitely many appropriate transformations of this type we get that $[\alpha; \beta]$ has the form

$$[0, \alpha_2, 0, \dots, 0; \beta_1, 0, \dots, 0] \quad \text{or} \quad [\alpha_1, \alpha_2, 0, \dots, 0; 0, 0, \dots, 0].$$

The second case is the desired form, so we leave it for the present and consider the first case. Now let x, y be any elements of R , and set

$$T(x) = \begin{bmatrix} I & 0 \\ xE_{12} + xE_{21} & I \end{bmatrix}, \quad V(y) = \begin{bmatrix} I & yE_{12} + yE_{21} \\ 0 & I \end{bmatrix}.$$

Then $T(x), V(y)$ are symplectic, and

$$\begin{aligned} [\alpha; \beta]T(x) &= [0, \alpha_2 + x\beta_1, 0, \dots, 0; \beta_1, 0, \dots, 0], \\ [\alpha; \beta]T(y) &= [0, \alpha_2, 0, \dots, 0; \beta_1 + y\alpha_2, 0, \dots, 0]. \end{aligned}$$

Again this sets up a euclidean algorithm, and after finitely many appropriate transformations of this type we get that $[\alpha; \beta]$ has the form

$$[0, \alpha_2, 0, \dots, 0; 0, 0, \dots, 0] \quad \text{or} \quad [0, 0, 0, \dots, 0; \beta_1, 0, \dots, 0].$$

Here the first form is the desired form, and the second may be put into the first by multiplication by the symplectic matrix $\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$. Hence, in *all* cases we can find a symplectic matrix S such that

$$[\alpha; \beta]S = [\alpha'; 0].$$

But α' is also primitive. Thus, α' may be completed to a unimodular matrix A . But then

$$T = \begin{bmatrix} A & 0 \\ 0 & (A^T)^{-1} \end{bmatrix}$$

is symplectic with first row $[\alpha'; 0]$, and TS^{-1} is symplectic with first row $[\alpha; \beta]$. This completes the proof.

PROOF OF THEOREM 3. Let π be any prime of R . By the results of [2, p. 128] we may determine a symmetric X such that $(\det(A + BX), \pi) = 1$. In particular, this means that $A + BX$ is nonsingular. Then $\begin{bmatrix} I & 0 \\ X & I \end{bmatrix}$ is symplectic, and

$$[A, B] \begin{bmatrix} I & 0 \\ X & I \end{bmatrix} = [A + BX, B].$$

Thus, we may assume that, originally, A is nonsingular (once again, we use the fact that if S is symplectic, then $[A, B]$ may be completed to a symplectic matrix if and only if $[A, B]S$ may be completed to a symplectic matrix). Similarly, we can also determine a symmetric Y such that $AY + B$ is nonsingular. Then $\begin{bmatrix} I & Y \\ 0 & I \end{bmatrix}$ is symplectic and

$$[A, B] \begin{bmatrix} I & Y \\ 0 & I \end{bmatrix} = [A, AY + B].$$

Thus, we may assume that, originally, *both* A and B are nonsingular.

Now again using the results of [2, p. 128], determine X symmetric so that $(\det(A + BX), \det(B)) = 1$. Arguing as before, this allows us to assume that, originally, A and B are nonsingular and $(\det(A), \det(B)) = 1$. Put $a = \det(A)$, $b = \det(B)$, and determine $a', b' \in R$ so that $aa' - bb' = 1$. Then $[A, B]$ has the symplectic completion

$$\begin{bmatrix} A & B \\ b'(B^T)^{\text{adj}} & a'(A^T)^{\text{adj}} \end{bmatrix},$$

where "adj" denotes the adjugate matrix. This completes the proof.

PROOF OF THEOREM 4. Since $[A, B]$ is primitive, matrices X, Y exist such that $AX - BY = I_p$, $X \in M_p$, $Y \in M_{q,p}$. We have (with Z as yet undetermined) $\det(M) = \det(N)$, where

$$\begin{aligned} N &= \begin{bmatrix} I & 0 \\ X^T & I \end{bmatrix} \begin{bmatrix} A & -BY \\ -Y^T B^T & Z \end{bmatrix} \begin{bmatrix} I & X \\ 0 & I \end{bmatrix} \\ &= \begin{bmatrix} I & 0 \\ X^T & I \end{bmatrix} \begin{bmatrix} A & I \\ -Y^T B^T & Z - Y^T B^T X \end{bmatrix} = \begin{bmatrix} A & I \\ I & Z + X^T - Y^T B^T X \end{bmatrix}. \end{aligned}$$

Now

$$X^T - Y^T B^T X = X^T - (X^T A - I)X = X + X^T - X^T A X,$$

which is symmetric. Thus, the choice $Z = X^T A X - X - X^T$ is permissible. For this choice N becomes

$$N = \begin{bmatrix} A & I \\ I & 0 \end{bmatrix}, \quad \det(N) = (-1)^p.$$

Hence, M is also unimodular and the proof is concluded.

PROOF OF THEOREM 5. We first note that if $U \in \text{GL}(t, R)$, $V \in \text{GL}(n - t, R)$, then

$$\begin{bmatrix} u & 0 \\ 0 & V \end{bmatrix} \begin{bmatrix} A & B \\ B^T & * \end{bmatrix} \begin{bmatrix} U^T & 0 \\ 0 & V^T \end{bmatrix} = \begin{bmatrix} UAU^T & UB V^T \\ VB^T U^T & * \end{bmatrix}.$$

Thus, $[A, B]$ has a symmetric completion if and only if $[UAU^T, UBV^T]$ has a symmetric completion. Thus, we may assume that, originally, B is in Smith normal form; and since $t \leq n - t$, we may assume that $[A, B] = [A, B_1, 0]$, where B_1 is $t \times t$, the zero block is $t \times (n - 2t)$, and $[A, B_1]$ must also be primitive. Furthermore, it suffices to consider only the extreme case when n is minimal, namely $n = 3t$, since the others may be reduced to this case by a simple argument involving direct sums with an identity matrix of appropriate size.

Since $[A, B_1]$ is primitive, there is a $2t \times 2t$ unimodular matrix

$$\begin{bmatrix} A & B_1 \\ * & * \end{bmatrix}.$$

Hence, the matrix

$$\begin{bmatrix} A & B_1 \\ * & * \end{bmatrix} \begin{bmatrix} I & 0 \\ -B_1^T & I \end{bmatrix} = \begin{bmatrix} A - B_1 B_1^T & B_1 \\ * & * \end{bmatrix}$$

is also unimodular. It follows that $[A - B_1 B_1^T, B_1]$ is primitive. In addition, $A - B_1 B_1^T$ is symmetric since A is symmetric. Set $A_1 = A - B_1 B_1^T$ and consider the $3t \times 3t$ matrix

$$M = \begin{bmatrix} A & B_1 & 0 \\ B_1^T & I_t & Y \\ 0 & Y & Z \end{bmatrix},$$

where the matrices Y, Z are yet to be determined, but must satisfy

$$(3) \quad Y, Z \in M_t, \quad Z = Z^T.$$

By applying elementary row operations we find that $\det(M) = \det(N)$, where

$$N = \begin{bmatrix} A_1 & 0 & -B_1 Y \\ B_1^T & I_t & Y \\ -Y^T B_1^T & 0 & Z - Y^T Y \end{bmatrix},$$

so that

$$\det(N) = \det \begin{bmatrix} A_1 & -B_1 Y \\ -Y^T B_1^T & Z - Y^T Y \end{bmatrix}.$$

Theorem 4 now implies that Y, Z may be determined so that (3) is satisfied and N is unimodular. But then M is symmetric and belongs to $\text{GL}(3t, R)$. This completes the proof.

As a supplement to this result, note that there are primitive elements $[A, B]$ of $M_{t, 2t}$ with A symmetric which do not have a $2t \times 2t$ completion. For example, choose $A = aI, B = bI$, where $(a, b) = 1$ and $b^{2t} \not\equiv \pm 1 \pmod{a}$. then if

$$M = \begin{bmatrix} A & B \\ B^T & X \end{bmatrix}, \quad X \in M_t,$$

$$\det(M) \equiv \det \begin{bmatrix} 0 & bI \\ bI & X \end{bmatrix} \equiv \pm b^{2t} \pmod{a},$$

so that M can never be unimodular.

PROOF OF THEOREM 6. Write $\alpha = [a, \beta]$, where $\beta \in M_{1, n-1}$. Let S be any element of $SL(n-1, R)$. We have

$$\begin{bmatrix} 1 & 0 \\ 0 & S^{-1} \end{bmatrix} \begin{bmatrix} a & \beta \\ * & \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & S \end{bmatrix} = \begin{bmatrix} a & \beta S \\ * & \end{bmatrix}.$$

Thus, it is sufficient to prove the theorem for the row $[a, \beta S]$, since conjugates of commutators are commutators. Choose S so that $\beta S = [b, 0, \dots, 0]$. Thus it is sufficient to prove that if $[a, b, 0]$ is a primitive element of $M_{1,3}$, then elements A, B of $SL(n, R)$ exist such that the first row of $ABA^{-1}B^{-1}$ is $[a, b, 0]$. This reduces the proof to a direct construction.

Let x, y be elements of R such that $ax + by = 1$. We have

$$\begin{aligned} & \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x & -b & 0 \\ y & a & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} a & b & 0 \\ -y & x & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & 1 \\ x & -b & 0 \\ y & a & 0 \end{bmatrix} \begin{bmatrix} -y & x & 0 \\ 0 & 0 & 1 \\ a & b & 0 \end{bmatrix} = \begin{bmatrix} a & b & 0 \\ -xy & x^2 & -b \\ -y^2 & xy & a \end{bmatrix}. \end{aligned}$$

This completes the proof, since

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} x & -b & 0 \\ y & a & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

both belong to $SL(3, R)$.

4. Some open questions. The results of this paper suggest a number of interesting questions. We list a few.

(a) Let G be a subgroup of $SL(n, R)$. Determine necessary and sufficient conditions for a primitive element α of $M_{1,n}$ to be completable to an element of G .

(b) Determine all subgroups G of $SL(n, R)$ such that every primitive element α of $M_{1,n}$ may be completed to an element of G .

(c) Determine all values of t such that $1 \leq t \leq n$, and if $A \in M_t$, $B \in M_{t, n-t}$, $A = A^T$, $[A, B]$ primitive, then $[A, B]$ may be completed to a symmetric matrix of $SL(n, R)$.

(d) Let R have the property that $SL(n, R)$ is its own commutator subgroup (for example, R a euclidean ring and $n > 2$). Determine whether or not an absolute constant c exists such that every element of $SL(n, R)$ is the product of at most c commutators.

REFERENCES

1. C. C. MacDuffee, *The theory of matrices*, Chelsea, New York, 1946.
2. M. Newman, *Integral matrices*, Academic Press, New York, 1972.
3. ———, *Symmetric completions and products of symmetric matrices*, Trans. Amer. Math. Soc. **186** (1973), 191–201.
4. I. Reiner, *Symplectic modular complements*, Trans. Amer. Math. Soc. **77** (1954), 498–505.
5. C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. (2) **36** (1935), 527–606.