Matrices of rational functions

W.A. Coppel

The properties of the degree of a matrix of rational functions are obtained in a simplified way, which enables them to be generalised to matrices whose elements are not necessarily rational functions. On the basis of these results a theory of realisations is developed, which similarly generalises the theory of state space realisations of a matrix of rational functions.

1. Introduction

In the application to control problems of spectral factorisation techniques two slightly different approaches have been used. The first, introduced by Popov [73] and further developed by Jakubovič [6], uses a controllability hypothesis to impose three conditions on the state space matrix $A$. The second, employed by Anderson [7] and Molinari [1], [12] for rather less general problems, uses the controllability hypothesis to impose only two of these conditions on $A$. The third condition, that $A$ have distinct eigenvalues, is avoided by using properties of the degree of a matrix of rational functions. The concept of degree was introduced by McMillan [9, 10], and has also been discussed by Duffin and Hazony [3] and Kalman [7]. In attempting to understand its role in these applications to control theory we have been led to an approach which enables the main properties of the degree to be developed very directly. (By means of Theorem 3 below the third condition on $A$ can be avoided also in the general problem of Popov-Jakubovič.)

However, the main merit of this approach is that it is no longer necessary to restrict attention to matrices of rational functions. With trivial changes the definition of determinantal denominators and Theorems

Received 8 April 1974.
1-5 in Section 2 hold equally well for matrices with elements from the quotient field of any unique factorisation domain (for example, the field of rational functions of several variables). Theorem 6 holds, more restrictively, for matrices with elements from the quotient field of any principal ideal domain (for example, the field of rational numbers).

The degree of a matrix of proper rational functions is equal to the minimum dimension of any state space realisation of the matrix. This raises the question whether the theory of state space realisations can also be embedded in a more general algebraic setting. Some results which suggest this possibility are stated in the original and stimulating book of Rosenbrock [14], but the proofs of these results make essential use of state space theory. In the remainder of the paper we develop a theory of realisations valid for matrices with elements in the quotient field of any principal ideal domain. This is not just a trivial exercise in generalisation and the logical order of development is quite different from that of Rosenbrock. Moreover, even in the rational function case our results extend his in some respects.

Nevertheless, to fix ideas and to make the contents of the paper more generally accessible, we will continue to talk throughout about polynomials and rational functions of one variable, with coefficients from an arbitrary ground field.

2. Determinantal denominators

Let $R$ be a $p \times m$ rational matrix. For any positive integer $k$ let $\varphi_k(R)$ denote the monic least common denominator of all minors of $R$ of order at most $k$. We also set $\varphi_0(R) = 1$ (since an 'empty' determinant has the value 1). The polynomials $\varphi_k(R)$ will be called the determinantal denominators of $R$.

Evidently $\varphi_k(R)$ divides $\varphi_{k+1}(R)$ for all $k \geq 0$. Also $\varphi_k(R) = \varphi_{k+1}(R)$ for $k \geq \min(p, m)$, in fact for $k \geq r = \text{rank} R$. For later use we define the width of $R$ to be the least non-negative integer $g$ such that $\varphi_k(R) = \varphi_{k+1}(R)$ for all $k \geq g$. The rational matrix $R$ has monic least denominator 1.
Matrices of rational functions

has width zero if and only if it is a polynomial matrix.

From the expression for a determinant as a polynomial in its elements we see that \( \varphi_k(R) \) divides \( [\varphi_1(R)]^k \) for all \( k \geq 0 \). More generally, by a Laplace expansion it may be seen that \( \varphi_{h+k}(R) \) divides \( \varphi_h(R)\varphi_k(R) \) for all \( h, k \geq 0 \).

**Theorem 1.** Let \( R_1 \) and \( R_2 \) be \( p \times m \) rational matrices, and let \( R = R_1 + R_2 \) be their sum. Then \( \varphi_k(R) \) divides \( \varphi_k(R_1)\varphi_k(R_2) \) for all \( k \).

If \( \varphi_1(R_1) \) and \( \varphi_1(R_2) \) are relatively prime then
\[
\varphi_k(R) = \varphi_k(R_1)\varphi_k(R_2)
\]
for all \( k \).

**Proof.** We need only consider the case \( 1 \leq k \leq \min(p, m) \). By linearity any \( k \times k \) minor \( \rho \) of \( R \) is a sum of \( 2^k \) determinants, each row of which is taken either from \( R_1 \) or from \( R_2 \). Consider one such determinant, with \( h \) rows taken from \( R_1 \) and \( k-h \) rows taken from \( R_2 \). By a Laplace expansion this determinant can be written as a sum of terms \( \pm \varphi_1 \varphi_2 \), where \( \varphi_1 \) is an \( h \times h \) minor of \( R_1 \) and \( \varphi_2 \) is a \((k-h)\times(k-h)\) minor of \( R_2 \). Hence \( \rho \) can be written with denominator \( \varphi_k(R_1)\varphi_k(R_2) \). It follows that \( \varphi_k(R) \) divides \( \varphi_k(R_1)\varphi_k(R_2) \).

Suppose \( \varphi_1(R_1) \) and \( \varphi_1(R_2) \) are relatively prime. Then \( \varphi_k(R_1) \) and \( \varphi_k(R_2) \) are also relatively prime. Since, by what we have already proved, \( \varphi_k(R_2) \) divides \( \varphi_k(\varphi_1(R_1))\varphi_k(R) \) it follows that \( \varphi_k(R_2) \) divides \( \varphi_k(R) \). Similarly \( \varphi_k(R_1) \) divides \( \varphi_k(R) \). Since they are relatively prime their product \( \varphi_k(R_1)\varphi_k(R_2) \) also divides \( \varphi_k(R) \). Hence
\[
\varphi_k(R) = \varphi_k(R_1)\varphi_k(R_2)
\]

**Theorem 2.** Let \( R_1 \) and \( R_2 \) be \( p \times n \) and \( n \times m \) rational matrices, and let \( R = R_1R_2 \) be their product. Then \( \varphi_k(R) \) divides \( \varphi_k(R_1)\varphi_k(R_2) \) for all \( k \).
Proof. Suppose first that \( 1 \leq k \leq q = \min(p, n, m) \). By the product formula for minors any \( k \times k \) minor \( \rho \) of \( R \) is a sum of terms \( \rho_1 \rho_2 \), where \( \rho_1 \) and \( \rho_2 \) are \( k \times k \) minors of \( R_1 \) and \( R_2 \). Hence \( \rho \) can be written with denominator \( \varphi_k(R_1) \varphi_k(R_2) \). It follows that \( \varphi_k(R) \) divides \( \varphi_k(R_1) \varphi_k(R_2) \).

Suppose next that \( k > q \). Then \( \varphi_k(R) = \varphi_q(R) \), since \( R \) has rank at most \( q \). Since the result holds for \( q \), it holds also for \( k \).

THEOREM 3. Let \( R_1 \) and \( R_2 \) be non-singular \( m \times m \) rational matrices, and let \( R = R_1 R_2 \) be their product. If \( \varphi_1(R_1) \) is relatively prime to \( \varphi_1(R_2) \) and to \( \varphi_1(R^{-1}) \), and if \( \varphi_1(R_2) \) is relatively prime to \( \varphi_1(R^{-1}) \), then \( \varphi_k(R) = \varphi_k(R_1) \varphi_k(R_2) \) for all \( k \).

Proof. By Theorem 2, \( \varphi_k(R) \) divides \( \varphi_k(R_1) \varphi_k(R_2) \). Since \( R_1 = RR_2^{-1} \) and \( \varphi_k(R_1) \) is relatively prime to \( \varphi_k(R_2^{-1}) \), it follows from Theorem 2 also that \( \varphi_k(R_1) \) divides \( \varphi_k(R) \). Since \( R_2 = R_1^{-1} R \) and \( \varphi_k(R_2) \) is relatively prime to \( \varphi_k(R_1^{-1}) \), it follows in the same way that \( \varphi_k(R_2) \) divides \( \varphi_k(R) \). Since \( \varphi_k(R_1) \) and \( \varphi_k(R_2) \) are relatively prime their product \( \varphi_k(R_1) \varphi_k(R_2) \) also divides \( \varphi_k(R) \). Hence \( \varphi_k(R) = \varphi_k(R_1) \varphi_k(R_2) \).

THEOREM 4. Let \( R \) be a non-singular \( m \times m \) rational matrix, and write \( \det R = \alpha/\beta \), where \( \alpha \) and \( \beta \) are polynomials. Then

\[
\beta \varphi_m(R^{-1}) = \alpha \varphi_m(R),
\]

where \( = \) denotes equality apart from a unit (non-zero constant) factor.

Proof. Any minor \( \tilde{\rho} \) of \( R^{-1} \) can be written in the form

\[
\tilde{\rho} = \tilde{\tau} \rho / \det R = \pm \beta \rho / \alpha,
\]

where \( \rho \) is the complementary minor of \( R \). The least common denominator

https://doi.org/10.1017/S0004972700043677 Published online by Cambridge University Press
of all $\bar{p}/\beta$ is $\beta \varphi_m(R^{-1})$. The least common denominator of all $\rho/\alpha$ is $\alpha \varphi_m(R)$. The result follows.

In particular, if $P$ is a non-singular $m \times m$ polynomial matrix then
\[ \varphi_m(P^{-1}) = \text{det}P. \]

**Theorem 5.** Let $R_1, R_2$ be $p_1 \times m_1, p_2 \times m_2$ rational matrices, and let $R = R_1 \oplus R_2$ be their direct sum. Then $\varphi_k(R)$ is the least common multiple of all products $\varphi_h(R_1)\varphi_{k-h}(R_2)$, where $0 \leq h \leq k$.

In particular, if $\varphi_1(R_1)$ and $\varphi_1(R_2)$ are relatively prime then $\varphi_k(R) = \varphi_k(R_1)\varphi_k(R_2)$ for all $k$.

Proof. Let $\chi_k(R)$ denote the least common multiple referred to in the statement of the theorem. Evidently $\chi_k(R)$ divides $\chi_{k+1}(R)$. It is sufficient to prove the theorem for $1 \leq k \leq \min(p_1 + p_2, m_1 + m_2)$.

Every non-zero $k \times k$ minor $\rho$ of $R$ is either a minor of $R_1$, or a minor of $R_2$, or a product $\rho_1\rho_2$, where $\rho_1$ is an $h \times h$ minor of $R_1$, $\rho_2$ is a $(k-h) \times (k-h)$ minor of $R_2$ and $0 < h < k$. In any case it can be written with denominator $\chi_k(R)$, and hence $\varphi_k(R)$ divides $\chi_k(R)$.

Consider a fixed value of $h$ ($0 \leq h \leq k$). Let $\pi$ be any prime polynomial and let $e_1, e_2$ be the highest powers of $\pi$ dividing $\varphi_h(R_1)$, $\varphi_{k-h}(R_2)$. Then there exists a minor $\rho_1$ of $R_1$ of order at most $h$ whose reduced denominator is divisible by $\pi^{e_1}$. Similarly there exists a minor $\rho_2$ of $R_2$ of order at most $k-h$ whose reduced denominator is divisible by $\pi^{e_2}$. We are going to show that there exists a minor $\rho$ of $R$ of order at most $k$ whose reduced denominator is divisible by $\pi^{e_1+e_2}$. If $e_1 > 0$, $e_2 = 0$ we can take $\rho = \rho_1$. If $e_1 = 0$, $e_2 > 0$ we can
take $\rho = \rho_2$. If $e_1 > 0$, $e_2 > 0$ we can take $\rho = \rho_1 \rho_2$. Since this holds for every prime $h$ it follows that $\phi_h(R_1)\phi_h(R_2)$ divides $\phi_h(R)$. Since this holds for every $h$ it follows that $\chi_h(R)$ divides $\phi_h(R)$. Hence $\phi_k(R) = \chi_k(R)$.

The determinantal denominators of a rational matrix will now be connected with its Smith McMillan normal form. Let $P$ be a $p \times m$ polynomial matrix of rank $r$. Then it is well-known (see Jacobson [5]) that there exist invertible $p \times p$, $m \times m$ polynomial matrices $A$, $B$ and monic polynomials $\gamma_1, \ldots, \gamma_r$ such that $\gamma_j$ divides $\gamma_k$ if $j \leq k$, for which

$$P = ACB,$$

where $c_{kk} = \gamma_k \quad (1 \leq k \leq r)$, $c_{ij} = 0$ otherwise.

The matrix $C$, known as the Smith normal form of $P$, is uniquely determined by $P$. In fact the product $\delta_k = \gamma_1 \cdots \gamma_k$ is the greatest common divisor of all $k \times k$ minors of $P$. The Smith normal form of $P$ will be denoted for short by $\{\gamma_1, \ldots, \gamma_r\}$.

In the next section we will have occasion to use the following known result.

**Lemma 1.** Let $P_1, P_2$ be $p \times n$, $n \times m$ polynomial matrices with the Smith normal forms $\{\gamma_1^{(1)}, \ldots, \gamma_r^{(1)}\}$, $\{\gamma_1^{(2)}, \ldots, \gamma_r^{(2)}\}$ respectively. If $P = P_1P_2$ has the Smith normal form $\{\gamma_1, \ldots, \gamma_r\}$ then $\gamma_k^{(1)}$ and $\gamma_k^{(2)}$ each divide $\gamma_k \quad (1 \leq k \leq r)$.

**Proof** (see Frobenius [4], pp. 577-590). The ranks satisfy the well-known inequality $r \leq \min(r_1, r_2)$. It will be sufficient to prove that $\gamma_k^{(1)}$ divides $\gamma_k$. For this purpose we may assume without loss of generality that $P_1$ is already in its Smith normal form. Put

---

2 A square polynomial matrix is invertible if and only if its determinant is a unit.
Matrices of rational functions

\[
\delta_k = \gamma_1 \ldots \gamma_k, \quad \delta_k^{(1)} = \gamma_1^{(1)} \ldots \gamma_k^{(1)} \quad (1 \leq k \leq r).
\]

If \( \rho \) is any non-zero \( k \times k \) minor of \( P \), corresponding to the rows \( i_1 < \ldots < i_k \), then since \( i_j \geq j \) the \( j \)-th row of \( \rho \) is divisible by \( \gamma_j^{(1)} \) for \( 1 \leq j \leq k \). Hence \( \rho \) is divisible by \( \delta_k^{(1)} \), and so the greatest common divisor \( \delta_k \) of all \( \rho \) is divisible by \( \delta_k^{(1)} \). This proves the assertion for \( k = 1 \). Now suppose \( k > 1 \). By expanding \( \rho \) according to the elements of its last row we see that it is divisible by \( \gamma_k^{(1)} \delta_{k-1} \), and so \( \delta_k \) is divisible by \( \gamma_k^{(1)} \delta_{k-1} \). This proves that \( \gamma_k^{(1)} \) divides \( \gamma_k \).

Now let \( R \) be a \( p \times m \) rational matrix of rank \( r \), and let \( \varphi = \varphi(R) \) be the monic least common denominator of all elements of \( R \). Then \( P = \varphi P \) is a polynomial matrix and hence has a Smith normal form \( \{ \gamma_1, \ldots, \gamma_r \} \). If we divide throughout by \( \varphi \) and express each rational function \( \gamma_k / \varphi \) in reduced form we obtain the representation

\[ R = ASB, \]

where \( A \) and \( B \) are invertible polynomial matrices,

\[ S = \{ \varepsilon_1 / \psi_1, \ldots, \varepsilon_r / \psi_r \}, \]

\( \varepsilon_k \) and \( \psi_k \) are relatively prime polynomials such that \( \varepsilon_j \) divides \( \varepsilon_k \) and \( \psi_j \) divides \( \psi_k \) if \( j \leq k \). It is easily shown (see McMillan \([9, 10]\)) that the matrix \( S \) is uniquely determined by these properties. It is known as the Smith McMillan normal form of \( R \).

**THEOREM 6.** Let \( R \) be a \( p \times m \) rational matrix with the Smith McMillan normal form \( \{ \epsilon_1 / \psi_1, \ldots, \epsilon_r / \psi_r \} \). Then

\[ \varphi_k(R) = \psi_1 \ldots \psi_k \quad \text{for} \quad 1 \leq k \leq r. \]

**Proof.** Let \( R = ASB \) as above. It follows from Theorem 2 that \( \varphi_k(R) \) divides \( \varphi_k(S) \), since \( \varphi_k(A) = \varphi_k(B) = 1 \). Since \( S = A^{-1}RB^{-1} \) it follows in the same way that \( \varphi_k(S) \) divides \( \varphi_k(R) \). Hence \( \varphi_k(R) = \varphi_k(S) \).

Thus it only remains to evaluate \( \varphi_k(S) \). We can regard \( S \) as the
direct sum of \( r \) \( 1 \times 1 \) matrices \( \{\psi_k/\psi_k^\psi\} \) and a matrix of zeros. It follows from Theorem 5 that \( \varphi_k(S) \) is the least common multiple of all products \( \psi_1 \cdots \psi_k \), where \( 1 \leq i_1 < \cdots < i_k \leq r \). But since \( \psi_j \) divides \( \psi_i \) if \( i \leq j \) this least common multiple is just \( \psi_1 \cdots \psi_k \).

3. Realisations

Let \( R \) be a \( p \times m \) rational matrix. A realisation of \( R \) is a representation of the form

\[
R = W + VTU,
\]

where \( W, V, T, U \) are polynomial matrices of size \( p \times m, p \times n, n \times n, n \times m \) and \( T \) is non-singular. The positive integer \( n \) will be called the dimension of the realisation. If \( R \) is actually a polynomial matrix it has the trivial and unique realisation \( R = R \) of dimension zero.

Any \( p \times m \) rational matrix \( R \) has a realisation of dimension \( \min(p, m) \). For let \( \varphi = \varphi_1(R) \) be the monic least common denominator of all elements of \( R \), so that \( \varphi R \) is a polynomial matrix. If \( p \geq m \) then

\[
R = O + \varphi R \varphi_1(R)_m^{-1} I_m.
\]

If \( m \geq p \) then

\[
R = O + I_p \varphi_1(R)_p^{-1} \varphi R.
\]

If \( R \) has the realisation (1) of dimension \( n \) then for any positive integer \( q \) it has the realisation

\[
R = W + (V P_q U)^{-1} U,
\]

of dimension \( n + q \).

Also, if \( R \) has the realisation (1) of dimension \( n \) then for any non-singular \( n \times n \) polynomial matrices \( D, \tilde{D} \) it has the realisation

\[
R = W + \tilde{D} D^{-1} DU.
\]
Matrices of rational functions

of the same dimension.

We now need some standard concepts concerning the divisibility of matrices. Let $T, U$ be $n \times l, n \times m$ polynomial matrices. An $n \times n$ polynomial matrix $D$ is said to be a common left divisor of $T$ and $U$ if there exist polynomial matrices $T_1, U_1$ such that

$$ T = DT_1, \quad U = DU_1. $$

The matrices $T, U$ are said to be left relatively prime if every common left divisor is invertible. It is easily seen that if there exist polynomial matrices $M, N$ such that

$$ TM + UN = I_n, $$

then $T, U$ are left relatively prime and the block matrix $(T U)$ has rank $n$.

A similar definition and result hold for right relatively prime matrices. One need only take transposes.

The realisation $(1)$ of $R$ will be said to be irreducible if $T, U$ are left relatively prime and $T, V$ are right relatively prime.

**THEOREM 7.** If the rational matrix $R$ has the realisation $(1)$ of dimension $n$ then it has an irreducible realisation

$$ R = W + V T_0^{-1} U_0 $$

of the same dimension, where

$$ T = DT_0 D, \quad U = DU_0, \quad V = V_0 D, $$

for some non-singular $n \times n$ polynomial matrices $D, D$.

Proof. Suppose $T$ and $U$ are not left relatively prime. Then

$$ T = D^{(1)} T^{(1)}, \quad U = D^{(1)} U^{(1)}, $$

where $D^{(1)}, T^{(1)}, U^{(1)}$ are polynomial matrices and $\det D^{(1)}$ is not a unit. If $T^{(1)}, U^{(1)}$ are not left relatively prime this process can be repeated. After $k$ steps we obtain

$$ T = D^{(1)} \ldots D^{(k)} T^{(k)}, \quad U = D^{(1)} \ldots D^{(k)} U^{(k)}, $$

https://doi.org/10.1017/S0004972700043677 Published online by Cambridge University Press
where \( \det D^{(1)}, \ldots, \det D^{(k)} \) are not units. Since \( \det T \) has only finitely many prime factors the process must terminate. That is, \( \hat{T} = T^{(k)} \) and \( U_0 = U^{(k)} \) are left relatively prime for some \( k \). Then

\[
T = DT, \quad U = DU_0,
\]

where \( D = D^{(1)} \ldots D^{(k)} \). In the same way we can write

\[
\hat{T} = T_0 \tilde{D}, \quad V = V_0 \tilde{D},
\]

where \( T_0 \) and \( V_0 \) are right relatively prime. Since \( \hat{T} \) and \( U_0 \) are left relatively prime it is clear that \( T_0 \) and \( U_0 \) must be also. The result follows.

**THEOREM 8.** Let \( T, U \) be \( n \times l, n \times m \) polynomial matrices which are left relatively prime and such that the block matrix \( (T \ A) \) has rank \( n \). Then there exists an \( (l+m) \times (l+m) \) invertible polynomial matrix \( A \) such that

\[
(T \ U)A = \begin{pmatrix} I_n & 0 \end{pmatrix}.
\]

Proof. Since the matrix \( (T \ U) \) has rank \( n \) there exist invertible \( n \times n, (l+m) \times (l+m) \) polynomial matrices \( X, Y \) such that

\[
X(T \ U)Y = (E 0),
\]

where \( E = \{e_1, \ldots, e_n\} \) is in Smith normal form. Hence

\[
(T \ U) = (D 0)Y^{-1},
\]

where \( D = X^{-1}E \). In terms of the partition

\[
Y^{-1} = \begin{bmatrix} Z_1 & Z_2 \\ Z_3 & Z_4 \end{bmatrix},
\]

corresponding to the partition \( (D 0) \), this means that

\[
T = DZ_1, \quad U = DZ_2.
\]

Since \( T, U \) are left relatively prime it follows that \( D \) is invertible. Taking
we obtain the theorem.

A more constructive approach to Theorems 7 and 8 is provided by the Hermite normal form (see MacDuffee [§, Chapter 3]). Since the matrix 
\((T U)\) has rank \(n\) an invertible \((l+m) \times (l+m)\) polynomial matrix \(Y\) can be found such that

\[(T U)Y = (D 0),\]

where the \(n \times n\) polynomial matrix \(D\) is lower triangular and nonsingular. Depending on \(Y\), the diagonal elements \(d_{jj}\) are uniquely determined apart from arbitrary unit factors and the subdiagonal elements \(d_{jk}\) with \(j > k\) are uniquely determined apart from arbitrary multiples of \(d_{jj}\). As in the proof of Theorem 8 we can write

\[T = D\hat{T}, \quad U = DU_0.\]

Moreover the polynomial matrices \(\hat{T}, U_0\) are left relatively prime, since

\[TY_1 + UY_3 = D.\]

If \(T, U\) are given left relatively prime then \(\det D\) is a unit. Hence the diagonal elements \(d_{jj}\) are all units, which we can take to be 1. Consequently the elements \(d_{jk}\) with \(j > k\) can be taken to be zero, so that \(D = I_n\).

**THEOREM 9.** Let \(R\) be a \(p \times m\) rational matrix with the realisation (1) of dimension \(n\). Suppose \(T, U\) are left relatively prime and let

\[A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}\]

be an invertible \((n+m) \times (n+m)\) polynomial matrix with the property described in Theorem 8; that is,

\[TA_1 + UA_3 = I_n,\]

\[TA_2 + UA_4 = 0_{n,m}.\]

If

\[A = \begin{pmatrix} D^{-1} & 0 \\ 0 & I \end{pmatrix},\]
\[ \tilde{V} = WA_4 - VA_2, \quad \tilde{T} = A_4, \]

Then \( \tilde{T} \) is non-singular and \( R \) has the realisation

\[ R = \tilde{V}^{-1} \]

of dimension \( m \).

If in addition \( T, V \) are right relatively prime, that is, if the realisation (1) is irreducible, then the realisation (2) is also irreducible. Moreover, if \( RY \) is a polynomial matrix for some polynomial matrix \( Y \), then \( Y = \tilde{T}X \) for some polynomial matrix \( X \).

Proof. We first note that since \( T \) is non-singular the block matrix \( (T U) \) certainly has rank \( n \). Let \( x \) be a polynomial \( m \)-vector such that \( A_i x = 0 \). Then \( TA_2 x = 0 \) and hence \( A_2 x = 0 \). Since \( A \) is non-singular (in fact invertible), it follows that \( x = 0 \). Thus \( \tilde{T} = A_4 \) is non-singular. Moreover

\[
\tilde{V} = WA_4 - VT^{-1}TA_2
= WA_4 + VT^{-1}UA_4
= RA_4.
\]

Suppose now that the realisation (1) is irreducible. Then, by Theorem 8, there exists an invertible \((n+p) \times (n+p)\) polynomial matrix

\[
B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}
\]

such that

\[
B_1 T + B_2 V = I_p, \\
B_3 T + B_4 V = 0_p, n.
\]

Let \( C = A^{-1} \) be partitioned in the same way as \( A \), so that

\[
C_3 A_2 + C_4 A_4 = I_m.
\]

Put

\[
M = -C_3 B_2, \quad N = C_4 - C_3 B_1 U + C_3 B_2 W.
\]
Matrices of rational functions

Then, by the definitions of \( \tilde{V} \) and \( \tilde{\tau} \),
\[
\tilde{M}\tilde{V} + N\tilde{\tau} = C_3 B_2 V A_2 + (C_4 - C_3 B_1 U) A_4
= C_3 (I - B_1 \tilde{T}) A_2 + C_4 A_4 + C_3 B_1 T A_2
= I_m.
\]

Thus \( \tilde{T}, \tilde{V} \) are right relatively prime, and the realisation (2) is irreducible. If \( Y \) is a polynomial matrix such that \( RY \) is also a polynomial matrix then
\[
\tilde{\tau}^{-1} Y = (M\tilde{\tau}^{-1} + N) Y
= (MR + N) Y
\]
is also a polynomial matrix. This completes the proof.

Considering still the irreducible case, let \( \tilde{T} \) be any \( m \times m \) polynomial matrix which shares the last property of \( \tilde{T} \), that is, \( R\tilde{T} \) is a polynomial matrix and if \( RY \) is a polynomial matrix for some polynomial matrix \( Y \) then \( Y = \tilde{T}X \) for some polynomial matrix \( X \). Then there exist polynomial matrices \( X_1, X_2 \) such that
\[
\tilde{T} = \tilde{T}X_1, \quad \tilde{\tau} = \tilde{T}X_2.
\]
Hence \( \tilde{T} = \tilde{T}X_1 X_2 \) and \( X_1 X_2 = I_m \). Thus \( \tilde{T} \) and \( \tilde{\tau} \) differ at most by an invertible right factor.

Again, suppose the \( p \times m \) rational matrix \( R \) has another realisation
\[
R = \tilde{V} \tilde{\tau}^{-1}
\]
of the same form. Then \( \tilde{V}_1 = R\tilde{T}_1 \) is a polynomial matrix and hence \( \tilde{T}_1 = \tilde{T}\tilde{X}_1 \) for some polynomial matrix \( \tilde{X}_1 \). It follows that \( \tilde{V}_1 = \tilde{V}\tilde{X}_1 \).

Hence the new realisation is irreducible if and only if \( \tilde{X}_1 \) is invertible.

The properties of determinantal denominators will now be applied to the theory of realisations.

**THEOREM 10.** Let \( R \) be a \( p \times m \) rational matrix with the realisation (1) of dimension \( n \). Then \( \varphi_k(R) \) divides \( \varphi_k(\tau^{-1}) \) for all \( k \).
If the realisation (1) is reducible then \( \varphi_n(R) \) is a proper divisor of \( \varphi_n(T^{-1}) \). If the realisation (1) is irreducible then \( \varphi_k(R) = \varphi_k(T^{-1}) \) for all \( k \).

Proof. By Theorem 1, \( \varphi_k(R) = \varphi_k(VT^{-1}U) \) and by Theorem 2, \( \varphi_k(VT^{-1}U) \) divides \( \varphi_k(T^{-1}) \). Thus \( \varphi_k(R) \) divides \( \varphi_k(T^{-1}) \).

Suppose \( T, U \) are not left relatively prime. Then we can write
\[
T = DT_1, \quad U = DU_1,
\]
where \( \det D \) is not a unit. Since
\[
R = W + VT^{-1}U_1,
\]
\( \varphi_n(R) \) divides \( \varphi_n(T_1^{-1}) \). But, by the corollary to Theorem 4,
\[
\varphi_n(T_1^{-1}) = \det T_1, \quad \varphi_n(T^{-1}) = \det T.
\]
Hence \( \varphi_n(R) \) is a proper divisor of \( \varphi_n(T^{-1}) \). The same conclusion is reached if \( T, V \) are not right relatively prime.

Suppose next that the realisation (1) is irreducible. Then, as shown in Theorem 8, there exist polynomial matrices \( A_1, A_3, B_1, B_2 \) such that
\[
TA_1 + UA_3 = I_n,
\]
\[
B_1T + B_2V = I_n.
\]
Thus
\[
T^{-1} = A_1 + T^{-1}UA_3,
\]
\[
T^{-1}U = B_1U + B_2VT^{-1}U.
\]
From the first equation \( \varphi_k(T^{-1}) = \varphi_k(T^{-1}UA_3) \) and hence \( \varphi_k(T^{-1}) \) divides \( \varphi_k(T^{-1}U) \). From the second equation \( \varphi_k(T^{-1}U) = \varphi_k(B_2VT^{-1}U) \) and hence
\( \varphi_k(T^{-1}u) \) divides \( \varphi_k(VT^{-1}u) \). Thus \( \varphi_k(T^{-1}) \) divides \( \varphi_k(VT^{-1}) = \varphi_k(R) \).

Therefore \( \varphi_k(R) = \varphi_k(T^{-1}) \).

**THEOREM 11.** Let \( R \) be a \( p \times m \) rational matrix. Then the width \( g \) of \( R \) is the minimal dimension of any realisation of \( R \).

**Proof.** Let \( R \) have the realisation (1) of dimension \( n \). By Theorem 7 we can suppose that this realisation is irreducible. Then, by the last part of Theorem 10, \( \varphi_k(R) = \varphi_{k+1}(R) \) for all \( k \geq n \). Hence \( n \geq g \).

It remains to show that there exists a realisation of dimension \( g \).

We can assume for this purpose that \( g > 0 \) and that \( R \) is in Smith McMillan form \( \{ \varepsilon_1/\psi_1, \ldots, \varepsilon_n/\psi_n \} \). Then, by Theorem 6, a realisation of \( R \) of dimension \( g \) is defined in the following way:

\[
W(p \times m) : \omega_{kk} = \varepsilon_k \text{ if } g < k \leq r , \quad \omega_{ij} = 0 \text{ otherwise},
\]

\[
V(p \times g) : \nu_{kk} = 1 \text{ if } 1 \leq k \leq g , \quad \nu_{ij} = 0 \text{ otherwise},
\]

\[
T(g \times g) : t_{kk} = \psi_k \text{ if } 1 \leq k \leq g , \quad t_{ij} = 0 \text{ otherwise},
\]

\[
U(g \times m) : \omega_{kk} = \varepsilon_k \text{ if } 1 \leq k \leq g , \quad \omega_{ij} = 0 \text{ otherwise}.
\]

This realisation is in fact irreducible (cf. the proof of Theorem 13).

**THEOREM 12.** Let \( R \) be a \( p \times m \) rational matrix of width \( g \), with the irreducible realisation (1) of dimension \( n \). If \( R \) has the Smith McMillan form \( \{ \varepsilon_1/\psi_1, \ldots, \varepsilon_n/\psi_n \} \) then \( T \) has the Smith form \( \{ I_{n-g}, \psi, \ldots, \psi \} \).

**Proof.** Let \( T \) have the Smith form \( \{ \tilde{\psi}_1, \ldots, \tilde{\psi}_g \} \). Then \( T^{-1} \) has the Smith McMillan form \( \{ 1/\tilde{\psi}_1, \ldots, 1/\tilde{\psi}_g \} \). By Theorem 10, \( \varphi_k(T^{-1}) = \varphi_k(R) \) for all \( k \). By Theorem 6,

\[
\varphi_k(T^{-1}) = \tilde{\psi}_1 \cdots \tilde{\psi}_k \text{ for } 1 \leq k \leq n ,
\]

\[
\varphi_k(R) = \psi_1 \cdots \psi_k \text{ for } 1 \leq k \leq r .
\]

The result now follows from Theorem 11.
If the realisation (1), of dimension \( n \), is not necessarily irreducible we can write \( T = DT_0D \), where \( T_0 \) belongs to an irreducible realisation of the same dimension. If \( T \) has the Smith form 
\[
\{ \tilde{\psi}_n', \ldots, \tilde{\psi}_1 \}
\] it follows from Lemma 1 that \( \psi_k \) divides \( \tilde{\psi}_k \) for \( 1 \leq k \leq g \). Apart from this restriction and the ordinary divisibility conditions the Smith form of \( T \) is arbitrary, even if we require either \( T, U \) to be left relatively prime or \( T, V \) to be right relatively prime. This may be seen by assuming \( T_0 \) in Smith form and multiplying by a suitable diagonal matrix.

Let \( R \) be a \( p \times m \) rational matrix with the realisation (1) of dimension \( n \). Then, following Rosenbrock [14], the \((n+p) \times (n+m)\) polynomial matrix

\[
P = \begin{bmatrix}
T & U \\
-V & W
\end{bmatrix}
\]

is called the system matrix of the realisation.

By direct multiplication it may be verified that

\[
P = \begin{bmatrix}
T & 0 \\
-V & I_p
\end{bmatrix}
\begin{bmatrix}
I_p^{-1} & 0 \\
0 & R
\end{bmatrix}
\begin{bmatrix}
T & U \\
0 & I_m
\end{bmatrix}.
\]

Hence \( P \) has rank \( n + r \).

That the system matrix is more than an array of coefficients is shown by the following result.

**THEOREM 13.** Let \( R \) be a \( p \times m \) rational matrix with the irreducible realisation (1) of dimension \( n \), and let \( P \) be the corresponding system matrix. If \( R \) has the Smith McMillan form 
\[
\{ \epsilon_1/\psi_1, \ldots, \epsilon_r/\psi_r \},
\]
then \( P \) has the Smith form 
\[
\{ I_n, \epsilon_1, \ldots, \epsilon_r \}.
\]

**Proof.** If \( \tilde{A}, \tilde{B} \) are invertible \( p \times p, m \times m \) polynomial matrices then \( \tilde{R} = \tilde{A}R\tilde{B} \) has the realisation

\[
\tilde{R} = \tilde{A}w\tilde{B} + \tilde{A}VT^{-1}U\tilde{B}
\]

with system matrix

\[
\tilde{P} = \begin{bmatrix}
I & 0 \\
0 & A
\end{bmatrix} P \begin{bmatrix}
I & 0 \\
0 & B
\end{bmatrix}.
\]
Therefore $\tilde{P}$ has the same Smith form as $P$. Moreover, since $\tilde{A}$ and $\tilde{B}$ are invertible, this realisation of $\tilde{R}$ is irreducible. Hence we can suppose that $R$ is already in its Smith McMillan form.

By Theorem 8 there exists an invertible $(n+m) \times (n+m)$ polynomial matrix

$$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$$

such that

$$(T U)A = \begin{pmatrix} I_n & 0 \\ 0 & W_1 \end{pmatrix}$$

Hence

$$PA = \begin{pmatrix} I_n & 0 \\ -V_1 & W_1 \end{pmatrix}$$

where

$$V_1 = VA_1 - WA_3,$$

$$W_1 = WA_4 - VA_2.$$  

Thus $P$ has the same Smith form as

$$\begin{pmatrix} I_n & 0 \\ 0 & W_1 \end{pmatrix}.$$  

Moreover, by Theorem 9, $R$ has the irreducible realisation

$$R = W_1A_4^{-1}.$$  

It also has the realisation $R = EF^{-1}$ defined by

$E(p \times m) : e_{kk} = \varepsilon_k$ (1 ≤ k ≤ r), $e_{ij} = 0$ otherwise,

$$F(m \times m) : f_{kk} = \psi_k$$(1 ≤ k ≤ r), $f_{kk} = 1$ (r < k ≤ m), $f_{ij} = 0$ (i ≠ j).

Since $\varepsilon_k$ and $\psi_k$ are relatively prime there exist 'diagonal' matrices $M, N$ such that

$$ME + NF = I_m.$$
Hence this realisation is also irreducible. Therefore, by the second remark following the proof of Theorem 9, \( E = W_1 \tilde{X}_1 \) for some invertible \( m \times m \) polynomial matrix \( \tilde{X}_1 \). Thus \( W_1 \) has the Smith form \( \{ \varepsilon_1, \ldots, \varepsilon_r \} \), and \( P \) has the Smith form \( \{ I_n, \varepsilon_1, \ldots, \varepsilon_r \} \). This completes the proof.

If the realisation (1), of dimension \( n \), is not necessarily irreducible, the corresponding system matrix \( P \) can be written in the form

\[
P = \begin{bmatrix} D & 0 \\ 0 & I \end{bmatrix} P_0 \begin{bmatrix} D & 0 \\ 0 & I \end{bmatrix},
\]

where \( P_0 \) is the system matrix of an irreducible realisation of the same dimension. If \( P \) has the Smith form \( \{ \tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_{n+p} \} \), it follows from Lemma 1 that \( \varepsilon_k \) divides \( \tilde{\varepsilon}_{n+k} \) for \( 1 \leq k \leq r \).

In Rosenbrock's treatment considerable use is made of the concept of strict system equivalence and attention is restricted to realisations of dimension not less than the degree of the polynomial \( \det T \) (which has no meaning outside the rational function case). The necessity for a restriction on the dimension is shown by the following simple example. The scalar rational function \( R(s) = (s+1)/s^2 \) has the 1-dimensional irreducible realisations defined by the system matrices

\[
\begin{bmatrix} s^2 & 1 \\ -s-1 & 0 \end{bmatrix}, \quad \begin{bmatrix} s^2 & s+1 \\ -1 & 0 \end{bmatrix}.
\]

However these realisations are not strictly system equivalent, since there do not exist polynomials \( x(s), n(s) \) such that

\[
1 = [s+1-s^2x(s)]n(s).
\]

We consider next some simple formal properties of realisations.

**Lemma 2.** Let \( R_1, R_2 \) be \( p \times m \) rational matrices with the realisations

\[
R_1 = W_1 + V_1 T_1^{-1} U_1, \quad R_2 = W_2 + V_2 T_2^{-1} U_2
\]

of dimension \( n_1, n_2 \) respectively. Then \( R = R_1 + R_2 \) has the realisation...
Matrices of rational functions

\[ R = W + VT^{-1}U \]

of dimension \( n_1 + n_2 \) defined by

\[ T = \begin{bmatrix} T_1 & 0 \\ 0 & T_2 \end{bmatrix}, \quad U = \begin{bmatrix} U_1 \\ U_2 \end{bmatrix}, \]

\[ V = \begin{bmatrix} V_1 & V_2 \end{bmatrix}, \quad W = W_1 + W_2. \]

The verification is immediate. Suppose \( \varphi_1(R_1) \) and \( \varphi_1(R_2) \) are relatively prime. Then, by Theorems 1 and 11,

\[ \varphi_{n_1+n_2}(R) = \varphi_{n_1+n_2}(R_1)\varphi_{n_1+n_2}(R_2) = \varphi_{n_1}(R_1)\varphi_{n_2}(R_2). \]

The realisation of \( R_1 \) is reducible if and only if \( \varphi_{n_1}(R_1) \) is a proper divisor of \( \det T_1 \). The realisation of \( R_2 \) is reducible if and only if \( \varphi_{n_2}(R_2) \) is a proper divisor of \( \det T_2 \). The realisation of \( R = R_1 + R_2 \) is reducible if and only if \( \varphi_{n_1+n_2}(R) \) is a proper divisor of \( \det T = \det T_1 \det T_2 \). It follows that the composite realisation of \( R = R_1 + R_2 \) is irreducible if and only if the realisations of \( R_1 \) and \( R_2 \) are both irreducible.

**Lemma 3.** Let \( R_1, R_2 \) be \( p \times n, n \times m \) rational matrices with the realisations

\[ R_1 = W_1 + V_1T_1^{-1}U_1, \quad R_2 = W_2 + V_2T_2^{-1}U_2 \]

of dimension \( n_1, n_2 \) respectively. Then \( R = R_1R_2 \) has the realisation

\[ R = W + VT^{-1}U \]

of dimension \( n_1 + n_2 \) defined by

\[ T = \begin{bmatrix} T_2 & 0 \\ -U_1 & V_1 \end{bmatrix}, \quad U = \begin{bmatrix} U_2 \\ U_1 \end{bmatrix}. \]
The verification is immediate. Suppose \( p = n = m \) and the hypotheses of Theorem 3 are satisfied. Then it follows as above that the composite realisation of \( R = R_1 R_2 \) is irreducible if and only if the realisations of \( R_1 \) and \( R_2 \) are both irreducible.

**Lemma 4.** Suppose the \( m \times m \) rational matrix \( R \) has a realisation \((1)\), of dimension \( n \), in which \( W \) is invertible. Then \( R \) is non-singular if and only if the polynomial matrix \( T + UW^{-1}V \) is non-singular.

In this case \( R^{-1} \) has the realisation

\[
R^{-1} = \tilde{W} + \tilde{V} T^{-1} \tilde{U},
\]

of the same dimension \( n \), defined by

\[
\tilde{T} = T + UW^{-1}V , \quad \tilde{U} = UW^{-1} , \\
\tilde{V} = -W^{-1}V , \quad \tilde{W} = W^{-1} .
\]

It is irreducible if and only if the realisation \((1)\) is irreducible.

**Proof.** Using a simple property of determinants (see Kalman [7], Lemma 5), we obtain

\[
\det \tilde{T} = \det T \cdot \det \left( I_n + T^{-1}UW^{-1}V \right) \\
= \det T \cdot \det \left( I_m + VT^{-1}UW^{-1} \right) \\
= \det T \cdot \det \left( W + VT^{-1}U \right) \cdot \det \left( W^{-1} \right) \\
= \det T \cdot \det R / \det W .
\]

This proves the first assertion. Define

\[
\tilde{R} = \tilde{W} + \tilde{V} T^{-1} \tilde{U} .
\]

Then

\[
\tilde{R} \tilde{R} = (W + VT^{-1}U) \left( \tilde{W} + \tilde{V} T^{-1} \tilde{U} \right) \\
= I_m + V \left( T^{-1} - T^{-1}UW^{-1}V T^{-1} \right) \tilde{U} \\
= I_m + VT^{-1} \left( T - UW^{-1}V \right) T^{-1} \tilde{U} \\
= I_m .
\]
Thus $\tilde{R} = R^{-1}$. Moreover $\varphi_n(R) = \varphi_m(R)$ is a proper divisor of $\det T$ if and only if the polynomial

$$
\varphi_n(R^{-1}) = \varphi_m(R^{-1}) \neq \det R \varphi_m(R)
$$

is a proper divisor of $\det \tilde{T} = \det R \det T$. The lemma follows.

By increasing the dimension of the realisation we can remove the restriction that $W$ be invertible. Let $R$ be a non-singular $m \times m$ rational matrix with the realisation (1) of dimension $n$ and corresponding system matrix $P$. Then, using (3), it is easily verified that $R^{-1}$ has the realisation

$$
R^{-1} = \hat{W} + \hat{V} \hat{T}^{-1} \hat{U},
$$

of dimension $n + m$, defined by

$$
\hat{T} = P, \quad \hat{U} = \begin{pmatrix} 0 \\ I_m \end{pmatrix},
$$

$$
\hat{V} = \begin{pmatrix} 0 & I_m \end{pmatrix}, \quad \hat{W} = 0.
$$

Moreover, since $\det \hat{T} = \det R \det T$ by (3), this realisation is irreducible if and only if the realisation (1) is irreducible.

It remains to establish the connection between the preceding theory and the concepts of degree and state space realisation. From now on we really do require the elements of our matrices to be rational functions.

Any $p \times m$ matrix $R(s)$ of rational functions can be uniquely expressed in the form

$$
R(s) = D(s) + R_0(s),
$$

where $D(s)$ is a matrix of polynomials and $R_0(s)$ is a matrix of proper rational functions. Let $\nu(R)$ denote the maximum degree of any of the polynomials $\varphi_k(R)$. Then the degree $\delta(R)$ may be defined by

$$
\delta(R) = \nu[D(s^{-1})] + \nu[R_0(s)].
$$

If $D(s)$ is a constant matrix then $\delta(R) = \nu(R)$. The properties of the degree can be deduced without difficulty from the theorems of Section 2.
In some applications, however, \( v(R) \) is more appropriate than \( \delta(R) \). The polynomials \( \varphi_k(R) \) convey more information than the integer \( v(R) \), and may be manipulated just as conveniently.

If the elements of \( R(s) \) are not all polynomials then a **state space realisation** of \( R(s) \) is a realisation of the form

\[
R(s) = D(s) + C(sI-A)^{-1}B
\]

where \( D(s) \) is the uniquely determined polynomial part of \( R(s) \) and \( A, B, C \) are constant matrices of size \( n \times n, n \times m, p \times n \). The theory of such realisations, due primarily to Kalman, is now widely known (see Brockett [2]).

The ordered pair \((A, B)\) is controllable if for some positive integer \( k \) the \( n \times km \) block matrix

\[
\Gamma = \begin{bmatrix} B & AB & \ldots & A^{k-1}B \end{bmatrix}
\]

has rank \( n \). The ordered pair \((A, C)\) is observable if \((A^*, C^*)\) is controllable. It is not difficult to show that a state space realisation (4) always exists, and furthermore that there exists one for which \((A, B)\) is controllable and \((A, C)\) is observable.

The following theorem is due to Rosenbrock, but the present proof is somewhat different.

**THEOREM 14.** Let \( A, B \) be \( n \times n, n \times m \) constant matrices. Then \((A, B)\) is controllable if and only if the polynomial matrices \( sI - A \) and \( B \) are left relatively prime.

**Proof.** Suppose first that \((A, B)\) is controllable and choose any positive integer \( k \) such that \( \Gamma \) has rank \( n \). Then there exist constant matrices \( Y_0, \ldots, Y_{k-1} \) such that

\[
BY_0 + ABY_1 + \ldots + A^{k-1}BY_{k-1} = I
\]

Put

\[
X_{j-1} = BY_j + ABY_{j+1} + \ldots + A^{k-j-1}BY_{k-1} \quad (1 \leq j < k).
\]

Then it is easily verified that
Matrices of rational functions

(5) \[ B\left[ Y_0 + sY_1 + \ldots + s^{k-1}Y_{k-1}\right] - (sI-A)\left[ X_0 + sX_1 + \ldots + s^{k-2}X_{k-2}\right] = I. \]

Thus \( sI - A \) and \( B \) are left relatively prime.

Conversely, suppose that \( sI - A \) and \( B \) are left relatively prime. Since \( sI - A \) is non-singular it follows from Theorem 8 that (5) holds for some positive integer \( k \) and constant matrices \( X_j, Y_j \). Equating coefficients we get

\[ BY_0 + AX_0 = I, \]
\[ BY_j + AX_j - X_{j-1} = 0 \quad (1 \leq j \leq k-2), \]
\[ BY_{k-1} - X_{k-2} = 0. \]

It follows that

\[ BY_0 + ABY_1 + \ldots + A^{k-1}BY_{k-1} = I. \]

Hence \( \Gamma \) has rank \( n \), and \((A, B)\) is controllable.

It follows that the state space realisation (4) is irreducible in the sense of the present paper if and only if \((A, B)\) is controllable and \((A, C)\) is observable. In this case, by Theorem 12, the polynomial matrix \( sI - A \) has Smith form \( \{I_{n-g}, \varphi/g\varphi_{g-1}, \ldots, \varphi_{1}/\varphi_0\} \), where \( \varphi_k = \varphi_k(R) \) and \( g \) is the width of \( R \). By standard results from linear algebra (see Jacobson [5], Chapter 3) it follows that the constant matrix \( A \) is similar to a direct sum of \( g \) companion matrices corresponding to the polynomials \( \varphi_1/\varphi_0, \ldots, \varphi_g/\varphi_{g-1} \).

Thus if the state space realisation is irreducible the determinantal denominators of \( R \) uniquely determine \( A \), apart from a similarity transformation which is inherent. In particular, the minimum polynomial of \( A \) is the least common denominator of all elements of \( R \), and the characteristic polynomial of \( A \) is the least common denominator of all minors of \( R \). Hence the realisation has dimension \( \nu(R) \).

ADDENDUM (24 May 1974). In Theorem 3 we have \( \varphi_m(R) = \varphi_m(R_1)\varphi_m(R_2) \) even without the hypothesis that \( \varphi_1(R_1) \) and \( \varphi_1(R_2) \) are relatively prime.

https://doi.org/10.1017/S0004972700043677 Published online by Cambridge University Press
Proof. From Theorem 4 and the relation \( \det R = \det R_1 \det R_2 \) we obtain
\[
(\ast) \quad \phi_m(R_1)\phi_m(R_2)\phi_m(R^{-1}) = \phi_m(R_1^{-1})\phi_m(R_2^{-1})\phi_m(R).
\]
Let \( \pi \) be any prime polynomial and let \( e_1, e_2 \) be its multiplicities as a divisor of \( \phi_m(R_1), \phi_m(R_2) \). We wish to show that \( e_1 + e_2 \) divides \( \phi_m(R) \). If \( e_1 > 0, e_2 = 0 \) this follows from the fact that \( \phi_m(R_1) \) divides \( \phi_m(R) \). If \( e_1 = 0, e_2 > 0 \), it follows from the fact that \( \phi_m(R_2) \) divides \( \phi_m(R) \). If \( e_1 > 0, e_2 > 0 \) it follows from (\ast) and the fact that \( \pi \) does not divide \( \phi_m(R_1^{-1}) \) or \( \phi_m(R_2^{-1}) \). Since \( \pi \) is arbitrary this proves that \( \phi_m(R_1)\phi_m(R_2) \) divides \( \phi_m(R) \), and hence \( \phi_m(R) = \phi_m(R_1)\phi_m(R_2) \).

Consequently the hypothesis that \( \phi_1(R_1) \) and \( \phi_1(R_2) \) are relatively prime may be omitted in the remark following Lemma 3. It is easily shown by examples that the full assertion of Theorem 3 does not hold when this hypothesis is omitted.

References


Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, ACT.