ACTA ARITHMETICA
XXV (1974)

A rational canonical form for matrix fields*

by

J. T. B. BEARD, JR., (Arlington, Tex.)

1. Introduction and notation. Let F be an arbitrary field and let $(F)_n$ denote the algebra of all $n \times n$ matrices over F under normal matrix addition and multiplication. The primary purpose of this paper is to examine a rational canonical form (R.C.F.) for matrix fields over F. This R.C.F. is in general not unique and the obvious questions remain open. In the final section we consider a relationship between matrix roots of prime polynomials over $\mathrm{GF}(q)$.

In certain instances we have a technique for extending matrix fields within $(F)_n$ ([1], Theorems 9, 10, [2], Theorems 12, 13). The R.C.F. defined in § 2 is principally motivated by an unsuccessful attempt to improve and generalize that technique. In particular we ask: given a subfield M of $(F)_n$ with M containing a matrix in rational canonical form (r.c.f.) over F, can we extend M non-trivially by adjoining a matrix $A \in (F)_n$ where A is in r.c.f. over F? The negative answer raises a more general question which we consider in § 3.

Our notation and terminology is that of [1], [2] and briefly is as follows. If a matrix $A \in (F)_n$ is the matrix direct sum of k companion matrices over F, we call A a *k-matrix* and follow the convention that the coefficients of a monic polynomial $f(x) \in F[x]$ determine the last row of its companion matrix $C(f(x))$. It is well known that if $g(x) = a_1x^{n-1} + \ldots + a_n \in F[x]$ and $C(f(x)) \in (F)_n$, then the first row of the matrix $g(C(f(x)))$ is given by the vector $(a_n, \ldots, a_1)$. By the r.c.f. over F of a matrix $A \in (F)_n$ we mean the matrix $\operatorname{diag}|C(f_1(x)), \ldots, C(f_k(x))|$, where the polynomials $f_i(x)$ are the non-trivial similarity invariants of A over F and $\deg f_i(x) \leqslant \deg f_{i+1}(x)$ for $1 \leqslant i < k$. Finally, we denote the set of all scalar matrices in $(F)_n$ by $S_n(F)$ and the set of all subfields of $(F)_n$ by $\mathscr{F}_n$.

2. A rational canonical form. We remember from [1] that if $M \in \mathscr{F}_n$ has rank r, then M is similar over F to a matrix field M' in which each matrix has the form $\operatorname{diag}|O_{n-r}, A'|$, and $A' \in (F)_r$ has rank r if and only

* Portions of this paper are contained in the author's doctoral dissertation, directed by Professor Robert M. McConnel.

if the corresponding matrix $A \in M$ is non-zero. We call M' a *normal form for* M *over* F and let $\pi_r M'$ denote the obvious projective image of M' in $\mathscr{F}_r$.

DEFINITION 1. Let $M \in \mathscr{F}_n$ have rank r and let M' be a normal form for M over F. Then M' is called a *rational canonical form* (R.C.F.) *for* M' *over* F if and only if $\pi_r M'$ contains a non-scalar matrix in r.c.f. over F whenever $\pi_r M'$ contains a non-scalar matrix.

Clearly, each $M \in \mathscr{F}_n$ having rank n is in normal form; $M' \in \mathscr{F}_n$ is its own unique R.C.F. whenever $\pi_r M'$ contains only scalar matrices; and each $M \in \mathscr{F}_n$ has a R.C.F. over F. While it is easy to verify that a R.C.F. is not necessarily unique, we are able to obtain the following theorem.

THEOREM 1. *Let F be an arbitrary field, and let $M \in \mathscr{F}_n$ have rank r. If M' is any R.C.F. for M over F, then $\pi_r M'$ contains at most one non-scalar matrix in r.c.f. over F.*

The above result follows immediately from Theorem 2.

THEOREM 2. *Let F be an arbitrary field, and let $M \in \mathscr{F}_n$ have rank n. Then at most one non-scalar matrix in M is in r.c.f. over F.*

Proof. Suppose M contains a non-scalar matrix A in r.c.f. over F, say

$$A = \mathrm{diag}|A_1, \ldots, A_k|,$$

where the companion matrix A_i has order m_i for $1 \leqslant i \leqslant k$. If $A' \in M$ is also a non-scalar matrix in r.c.f. over F, we let

$$A' = \mathrm{diag}|A'_1, \ldots, A'_l|,$$

where the companion matrix A'_i has order n_i for $1 \leqslant i \leqslant l$. Since neither A nor A' are scalar matrices, then $k, l < n$. Let π and π' denote the ordered partitions of n as defined by $(m_1, \ldots, m_k)$ and $(n_1, \ldots, n_l)$ respectively. Let $m = \max(m_k, n_l)$. We can assume w.l.o.g. that m belongs to the partition π. Partition both A and A' into block matrices, say $A = |B_{ij}|$ and $A' = |B'_{ij}|$, where B_{ij} and B'_{ij} both have dimensions $m_i \times m_j$ for $1 \leqslant i, j \leqslant k$, as determined by the partition π. Then $A_k = B_{kk}$ is non-derogatory. Since M is a field, A and A' commute. We conclude that B_{kk} commutes with B'_{kk}, and hence that $B'_{kk} = g(B_{kk})$ for some $g(x) \in F[x]$ with $\deg g(x) < m = m_k$. Since B_{kk} is a companion matrix it follows that $g(x) = a$ for some $a \in F$ or else $g(x) = x$, due to the form of the first row of B'_{kk}. If $g(x) = a$ then $A'_l = |a|$, and hence $A' = aI_n$ by the divisibility properties of the similarity invariants of A'. This is a contradiction, hence $g(x) = x$ and $A_k = A'_l$. Thus $A = A'$, for otherwise $A - A'$ is non-zero and has rank less than n.

In summary, we have

THEOREM 3. *Let F be an arbitrary field, and let $M \in \mathscr{F}_n$ have rank r. Then M has a R.C.F. over F. If $M' \in \mathscr{F}_n$ is any R.C.F. for M over F and K is any extension field over F, then M' is a R.C.F. for M over K. Furthermore, $\pi_r M'$ contains at most one non-scalar matrix in r.c.f. over F.*

3. k-matrices in matrix fields.

The proof technique used in Theorem 2 does not appear to be particularly fragile, so we question the uniqueness of k-matrices in matrix fields. The answer is negative as shown by this example.

EXAMPLE. Let $F = \mathrm{GF}(64)$ so that F has prime subfield $\mathrm{GF}(2)$ and proper subfields $\mathrm{GF}(4)$ and $\mathrm{GF}(8)$. Let $f(x) = x^2 + x + 1$, so that $f(x)$ is prime in $\mathrm{GF}[2, x]$ and splits over $\mathrm{GF}(4)$. Choose $a_1 \in \mathrm{GF}(4)$ as a root of $f(x)$. Let $C_1 = C(f(x))$, $A_1 = a_1 I_3$ where I_3 is the identity of $(F)_3$, and $A = \mathrm{diag}|C_1, A_1|$. Then $S_5(\mathrm{GF}(2))[A] \in \mathscr{F}_5$.

Now let $g(x) = x^3 + x + 1$, so that $g(x)$ is prime in $\mathrm{GF}[2, x]$ and splits over $\mathrm{GF}(8)$, and choose a root a_2 of $g(x)$ in $\mathrm{GF}(8)$. Let $A_2 = C(g(x))$, $C_2 = a_2 I_2$, and $B = \mathrm{diag}|C_2, A_2|$. It follows that $S_5(\mathrm{GF}(2))[A, B] \in \mathscr{F}_5$ and contains the non-scalar 4-matrix A, and also the non-scalar 3-matrix B.

In the other direction, it is easy to construct matrix fields in which the zero matrix is the only k-matrix.

We do gain the desired uniqueness in certain cases and are reminded of the question in [2] concerning the set of scalar matrices contained in a matrix field. We remember that if T is a subset of $(F)_n$, then the *entry field* of T is the smallest subfield F' of F such that T is contained in $(F')_n$. The method of Theorem 2 yields the following result.

THEOREM 4. *Let F be an arbitrary field. Let $M \in \mathscr{F}_n$ be in normal form having rank r and entry field F', and suppose $\pi_r M$ contains $S_r(F')$. If M contains a k-matrix A and an l-matrix A' with $k, l < n$, then $A = A'$.*

4. Other results.

In this section we sharpen and extend the following result.

THEOREM 5. *Let $F = \mathrm{GF}(p)$. Let $A \in (F)_n$ have characteristic polynomial $f^k(x)$ and minimal polynomial $f(x)$ which is prime in $F[x]$. Then for each positive divisor m of n/k there exists a polynomial $g(x) \in F[x]$ of degree $r < n/k$ and a prime polynomial $h(x) \in F[x]$ of degree m such that $g(A)$ has characteristic polynomial $h^{n/m}(x)$ and minimal polynomial $h(x)$.*

The above theorem will follow easily from Theorem 2 in [1]. We remember that if $F = \mathrm{GF}(q)$ is the Galois field of order q and $A \in (F)_n$ has minimal polynomial of degree m over F, then the ring extension $S_n(F)[A]$ of $S_n(F)$ by A has order q^m and is given by

$$S_n(F)[A] = \{g(A)\colon g(x) \in F[x], \deg g(x) < m\}.$$

We restate Theorem 5 equivalently but in simpler form.

THEOREM 6. *Let $F = \mathrm{GF}(p)$. Suppose $A \in (F)_n$ has minimal polynomial $f(x)$ which is prime in $F[x]$ and has degree s. Then for each positive* *divisor m of s, there exists a polynomial $g(x) \in F[x]$ of degree $r < s$ and a prime polynomial $h(x) \in F[x]$ of degree m, such that $g(A)$ has minimal polynomial $h(x)$.*

Proof. The ring $S_n(F)[A]$ is a subfield of $(F)_n$ by Theorem 2 in [1], since A has the matrix k-sum$\big(C(f(x))\big)$ as its rational canonical form over F, where $k = n/s$. Since $m|s$ then $S_n(F)[A]$ has a subfield M of order p^m. Since $S_n(F)$ is a prime field then $M = S_n(F)[B]$ for some $B \in S_n(F)[A]$. Let $h(X) \in S_n(F)[X]$ be the minimal polynomial of B over $S_n(F)$. Then $h(x)$ is the minimal polynomial of B over F, and we can choose (uniquely) $g(x) \in F[x]$ such that $\deg g(x) < s$ and $g(A) = B$.

We now sharpen the above result.

THEOREM 7. *Let $F = \mathrm{GF}(p)$. Suppose $A \in (F)_n$ has minimal polynomial $f(x)$ which is prime in $F[x]$ and has degree s. Then for each positive divisor m of s and for each prime polynomial $h(x) \in F[x]$ of degree m, there exist precisely m polynomials $g_i(x) \in F[x]$ of degrees $r_i < s$ such that $g_i(A)$ has minimal polynomial $h(x)$.*

Proof. As before, the field $S_n(F)[A]$ has order p^s and contains a subfield $S_n(F)[B]$ of order p^m. As argued in the proof of Theorem 2 in [3], any prime polynomial $h(x) \in F[x]$ of degree m splits in $S_n(F)[B]$. The theorem follows easily.

As indicated by Section 6 of [3], there is now no difficulty in obtaining a more general result.

THEOREM 8. *Let $F = \mathrm{GF}(q)$. Suppose $A \in (F)_n$ has characteristic polynomial $f^k(x)$ and minimal polynomial $f(x)$ which is prime in $F[x]$. Then for each positive divisor m of n/k and each prime polynomial $h(x) \in F[x]$ of degree m, there exist precisely m polynomials $g_i(x) \in F[x]$ of degrees $r_i < n/k$ such that $g_i(A)$ has characteristic polynomial $h^{n/m}(x)$ and minimal polynomial $h(x)$.*

Our next result follows from the proof of Theorem 20 in [3].

THEOREM 9. *Let $F = \mathrm{GF}(q)$, $q = p^d$. Suppose $A \in (F)_n$ is a root of a polynomial $f(x)$ which is prime in $\mathrm{GF}[p, x]$ and has degree s. Then for each positive divisor m of s, and for each polynomial $h(x)$ of degree m which is prime in $\mathrm{GF}[p, x]$ and has a root in $(F)_n$, there exist precisely m polynomials $g_i(x) \in \mathrm{GF}[p, x]$ of degrees $r_i < s$ such that $g_i(A)$ has minimal polynomial $h(x)$ over $\mathrm{GF}(p)$.*

Proof. Since $f(x)$ is prime in $\mathrm{GF}[p, x]$ then $f(x)$ is the minimal polynomial of A over $\mathrm{GF}(p)$, and $M = S_n\big(\mathrm{GF}(p)\big)[A]$ is a field of order p^s. Hence M contains a subfield $S_n\big(\mathrm{GF}(p)\big)[B]$ of order p^m where $B \in M$. Again, any polynomial $h(x)$ of degree m which is prime in $\mathrm{GF}[p, x]$ and has a root in $(F)_n$ splits in $S_n\big(\mathrm{GF}(p)\big)[B]$.

We can obtain results in the "opposite direction" by modifying appropriately the constructive technique of Theorem 9 in [1] or more generally Theorem 12 in [2]. For example, consider the following

THEOREM 10. *Let $F = \mathrm{GF}(q)$. Suppose $A \in (F)_n$ has characteristic polynomial $f^k(x)$ and minimal polynomial $f(x)$ which is prime in $F[x]$. Then for each positive integer m such that $m|k$ and for each prime polynomial $h(x) \in F[x]$ of degree mn/k, there exist at least mn/k matrices $B_i \in (F)_n$ having characteristic polynomial $h^{k/m}(x)$, minimal polynomial $h(x)$, and satisfying $A = g_i(B_i)$ for unique $g_i(x) \in F[x]$ of degrees $r_i < mn/k$.*

References

[1] J. T. B. Beard, jr., *Matrix fields over prime fields*, Duke Math. J. 39 (1972), pp. 313–322.

[2] — *Matrix fields over finite extensions of prime fields*, Duke Math. J. 39 (1972), pp. 475–484.

[3] — *The number of matrix fields over* GF(q), Acta Arith., this volume, pp. 315–329)

UNIVERSITY OF TEXAS AT ARLINGTON
Arlington, Texas

Received on 30. 5. 1972 (291)