MATRIX FIELDS OVER FINITE EXTENSIONS OF PRIME FIELDS

J. T. B. BEARD, JR.

1. Introduction and notation. Let F be a field and let $(F)_n$ denote the algebra of all $n \times n$ matrices over F under normal matrix addition and multiplication. Let M be any subring of $(F)_n$ such that M itself is a field. Then M is called a *matrix field* of $(F)_n$ or simply a *matrix field*. In addition, although it is nonstandard, we find it convenient to refer to M as a subfield of the ring $(F)_n$. We continue the work begun in [1], and in this paper we are primarily interested in characterizing all subfields of $(F)_n$ when F is a finite extension of its prime subfield F_p, p either a prime or zero.

Our notation and language is that of [1] and briefly is as follows. Unless stated otherwise, F denotes an arbitrary field. Polynomials over F are denoted by $f(x)$, $g(x)$, $\cdots$ and the degree of $f(x)$ is denoted by $\deg f(x)$. If $f(x)$ is monic and irreducible over F, we say that $f(x)$ is prime in $F[x]$. Capital letters are used to denote matrices unless otherwise noted, and we will have occasion to use the notation $A = |a_{ij}|$ also (No confusion will result as determinants are not used.). The usual terminology regarding matrices is used, and we assume the following facts. These are well-known and appear in standard texts on matrix algebra unless otherwise referenced. In particular, we have adopted the notation and language of Perlis [4]. While some of these facts are elementary, we rely on each of them heavily.

FACT 1. *Each matrix* $A \in (F)_n$ *is similar over* F *to a matrix* $C \in (F)_n$ *of the form* $C = \operatorname{diag} |C(f_1(x)), \cdots, C(f_k(x))|$, *where* $C(f_i(x))$ *denotes the companion matrix of* $f_i(x) \in F[x]$ *for* $1 \leq i \leq k$ *and where*

(i) $f_1(x), \cdots, f_k(x)$ *are the nontrivial similarity invariants of* A,

(ii) $0 < \deg f_i(x) \leq \deg f_{i+1}(x)$ *for* $1 \leq i < k$,

(iii) $f_i(x) \mid f_{i+1}(x)$ *in* $F[x]$ *for* $1 \leq i < k$,

(iv) $f_k(x)$ *is the minimal polynomial of* A *over* F, *and*

(v) $f(x) = \prod_{i=1}^{k} f_i(x)$ *is the characteristic polynomial of* A.

We follow Parker and Eaves [3] and refer to the matrix C in Fact 1 as the rational canonical form for A over F.

FACT 2. *Given any nonsingular matrix* $P \in (F)_n$ *the mapping* $\phi: (F)_n \to (F)_n$ *defined by* $\phi(A) = PAP^{-1}$ *for all* $A \in (F)_n$ *is a ring automorphism of* $(F)_n$.

We refer to the mapping ϕ in Fact 2 as a similarity transformation over F. If T is any subset of $(F)_n$, then we say that T and $\phi(T)$ are similar over F and that $\phi(T)$ is the conjugate of T by P.

Received November 18, 1971. Revision received April 24, 1972. This research was partially supported by NSF Grant GP-7129. A major portion of this paper is contained in the author's doctoral dissertation directed by Robert M. McConnel, to whom the author wishes to express his sincere gratitude.