# MATRIX FIELDS OVER $GF(q)$

MICHAEL WILLETT

**1. Introduction.** Beard [1], [2] has characterized all subsets $M$ of $n \times n$ matrices over a field $F$ (with $F$ prime or a finite extension of a prime field) which are fields. In the special case that $F$ is a finite field, we find an alternate characterization in terms of primitive polynomials to be more useful, especially in the construction of such fields. The purpose of this note then is to characterize all matrix fields over finite fields and to illustrate the construction of such fields.

**2. Preliminaries.** Let $F = GF(q)$, $q = p^s$ for some prime $p$, be a Galois field of $q$ elements, let $(F)_n$ be the set of all $n \times n$ matrices over $F$, and let $F_n$ be the collection of all subsets of $(F)_n$ which are fields with the usual matrix addition and multiplication. Since the set of all scalar matrices over $F$ forms a field, $F_n$ is nonempty. Let the zero matrix be denoted by $[0]$ and the $n \times n$ identity matrix by $I_n$. Let

$$f(x) = x^k - a_1x^{k-1} - \cdots - a_k \tag{1}$$

be a monic polynomial of degree $k$ over $F$. To be precise in out later work we point out that a monic polynomial is one whose leading coefficient, very often not written, is the multiplicative identity of the field. If a root of $f(x)$ in the finite extension $GF(q^k)$ of $F$ generates the multiplicative group of $GF(q^k)$, then $f(x)$ is called a primitive polynomial. There are $\phi(q^k - 1)/k$ such polynomials over $F$, where $\phi$ is Euler's function. The following is well known.

LEMMA 1. *The following are equivalent.*

(i) *$f(x)$ is primitive over $F$.*

(ii) *Any nontrivial solution over $F$ to the linear recursion*

$$u_{t+k} = a_1u_{t+k-1} + \cdots + a_ku_t\,, \qquad t = 0, 1, 2, \cdots, \tag{2}$$

*has minimum period $q^k - 1$.*

(iii) min $\{e > 0 \mid f(x)$ *divides* $x^e - 1\} = q^k - 1$.

(iv) *If $C(f)$ is the $k \times k$ companion matrix for $f(x)$, then*

$$\min \{e > 0 \mid [C(f)]^e = I_k\} = q^k - 1.$$

(v) *(Ore-Gleason-Marsh)*

$$g(x) \equiv x^{q^k-1} - a_1x^{q^{k-1}-1} - a_2x^{q^{k-2}-1} - \cdots - a_k$$

*is irreducible over $F$.*

Received March 19, 1973.