Finite Fields and Their Applications 46 (2017) 280–303

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Existence of some special primitive normal elements over finite fields

Anju *, R.K. Sharma

Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, 110016, India

ARTICLE INFO

Article history:
Received 29 December 2016
Received in revised form 7 April 2017
Accepted 10 April 2017
Available online xxxx
Communicated by D. Panario

MSC:
12E20
11T23

Keywords:
Finite field
Character
Normal element
Primitive element

ABSTRACT

In this article, we establish a sufficient condition for the existence of a primitive element $\alpha \in \mathbb{F}_q$ such that for any matrix $\begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_q)$ of rank 2, the element $(a\alpha^2 + b\alpha + c)/(d\alpha + e)$ is a primitive element of $\mathbb{F}_q$, where $q = 2^k$ for some positive integer k. We also give a sufficient condition for the existence of a primitive normal element $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that $(a\alpha^2+b\alpha+c)/(d\alpha+e)$ is a primitive element of $\mathbb{F}_{q^n}$ for every matrix $\begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_{q^n})$ of rank 2.

1. Introduction

Throughout the paper, $\mathbb{F}_q$ denotes a finite field of order $q = p^k$, for some prime p and some positive integer k, and $\mathbb{F}_{q^n}$ denotes an extension of $\mathbb{F}_q$ of degree n. A generator of the cyclic multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is known as a *primitive element* of $\mathbb{F}_q$. Any

* Corresponding author.
E-mail addresses: anjugju@gmail.com (Anju), rksharmaiitd@gmail.com (R.K. Sharma).

http://dx.doi.org/10.1016/j.ffa.2017.04.004
1071-5797/

field $\mathbb{F}_q$ has $\phi(q-1)$ primitive elements, where ϕ is the Euler's phi-function. A basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is called a *normal basis*, and α is called a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If, in addition, α is also a primitive element of $\mathbb{F}_{q^n}$, then the basis is said to be a *primitive normal basis*. Normal bases are of great importance in coding theory, cryptography, signal processing, etc. [1,18,19]. It is well known [17, Theorem 2.35], that $\mathbb{F}_{q^n}$ has a normal element over $\mathbb{F}_q$ for every q and n. Basic results on normal bases over finite fields can be found in [2].

Existence of primitive normal elements has become an active area of research because of applications in coding theory, cryptography, etc. In [3,4], Carlitz showed that for sufficiently large q^n, the field $\mathbb{F}_{q^n}$ contains a primitive element that generates a primitive normal basis over $\mathbb{F}_q$. Davenport [11] proved the existence of a primitive normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ when q is a prime. Lenstra and Schoof [15] completely resolved the question of the existence of primitive normal elements for all field extensions $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Cohen and Huczynska [9] gave the first computer-free proof of the result of Lenstra and Schoof.

In general, for any primitive element $\alpha \in \mathbb{F}_q$, $f(\alpha)$ (where f is any rational function) need not be primitive in $\mathbb{F}_q$, for example, if we take the polynomial function $f(x) = x+1$ over the field $\mathbb{F}_2$ of order 2 then 1 is the only primitive element of $\mathbb{F}_2$, but $f(1) = 0$, which is not primitive. But for $f(x) = \frac{1}{x}$, $f(\alpha)$ is primitive in $\mathbb{F}_q$ whenever α is primitive. We call $(\alpha, f(\alpha))$ a *primitive pair* if both α and $f(\alpha)$ are primitive. Many researchers have worked in this direction. In 1985, Cohen [7] showed that a finite field $\mathbb{F}_q$, with $q > 3$, $q \not\equiv 7(mod\ 12)$ and $q \not\equiv 1(mod\ 60)$ contains two consecutive primitive elements. Tian and Qi [20] showed the existence of a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that both α and α^{-1} are normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, when $n \geq 32$. Later, Cohen and Huczynska [10] proved that for any prime power q and any integer $n \geq 2$, there exists an element $\alpha \in \mathbb{F}_{q^n}$ such that both α and α^{-1} are primitive normal over $\mathbb{F}_q$ except when (q, n) is one of the pairs $(2,3)$, $(2,4)$, $(3,4)$, $(4,3)$, $(5,4)$. Chou and Cohen [6] completely resolved the question whether there exists a primitive element α such that α and α^{-1} both have trace zero over $\mathbb{F}_q$. In 2014, Kapetanakis [14] extended the result of Cohen and Huczynska [10] by proving the existence of a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that both α and $(a\alpha + b)/(c\alpha + d)$ produce a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, for every q, n, with a few exceptions, and for every a, b, c, $d \in \mathbb{F}_q$. He and Han [12] studied primitive elements of the form $\alpha + \alpha^{-1}$ over finite fields. In 2012, Wang et al. [21] gave a sufficient condition for the existence of α such that α and $\alpha + \alpha^{-1}$ are both primitive, and also a sufficient condition for the existence of a normal element α such that α and $\alpha + \alpha^{-1}$ are both primitive for the case $2|q$. Liao et al. [16] generalized their results to the case when q is any prime power. In 2014, Cohen [8] completed the existence results obtained by Wang et al. [21] for finite fields of characteristic 2. In this article, we extend results of Wang et al. and of Cohen.

Corresponding to every matrix $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_q)$, we define a rational expression $\lambda_A(x) \in \mathbb{F}_q(x)$ and a subset $\mathfrak{M}_q$ of $M_{2\times 3}(\mathbb{F}_q)$ given by